MICROSOFT SQL SERVER
DATABASE SECURITY CHECKLIST

Version 8, Release 1.2

26 June 2009

Developed by DISA for the DOD

UNCLASSIFIED

This page is intentionally left blank.

TABLE OF CONTENTS

1. Introduction

1.1 Overview

The SQLServer Database Security Readiness Review (SRR) targets conditions that undermine the integrity of security, contribute to inefficient security operations and administration, or may lead to interruption of production operations. Additionally, the review ensures the site has properly installed and implemented the database environment and that it is being managed in a way that is secure, efficient and effective. The items reviewed are derived from the general requirements listed in the Database Security Technical Implementation Guide (STIG) as they apply to a SQL Server installation. The Database STIG requirements are in turn derived from DOD policy documents, most notably, Department of Defense (DOD) Directive 8500.1 and DOD Instruction 8500.2 and the Information Assurance (IA) Controls defined therein. This document and the security check procedures it provides are intended to be used to measure compliance with the security requirements listed in the Database STIG. Please see the Database STIG for additional security explanation and discussion to assist in understanding the nature of the security requirements.

Each security item to review is listed in this document with a procedure for measuring compliance with the security requirement. The result of the procedure is a status of compliance with the requirement. Results are assigned as one of the following:

O = Open finding or non-compliance
NF = Not a Finding or in compliance
NA = Not Applicable or the item is not applicable to the database version, database use or host platform being reviewed
NR = Not Reviewed or the procedure was not completed so compliance is not determined
MR = Manual review. Can be the following check types:

1. Interview – Requires information found outside the DBMS
2. Manual – Requires information that cannot be automated
3. Verify – Requires verification of information found in the DBMS

DISA Field Security Operations (FSO) has assigned a level of urgency to each finding based on Chief Information Officer (CIO) established criteria for certification and accreditation. All findings are based on regulations and guidelines. All findings require correction by the host organization. Category I findings are any vulnerabilities that provide an attacker immediate access into a machine, super user access, or access that bypasses a firewall. Category II findings are any vulnerabilities that provide information that has a high potential of giving access to an intruder. Category III findings are any vulnerabilities that provide information that potentially could lead to compromise.

Note: Security patches required by the DOD IAVM process are reviewed during an operating system security review.

1.2 Organization of the Checklist

The Database Security Checklist is composed of five major sections and three appendices. The organizational breakdown proceeds as follows:

Section 1	Introduction
	This section contains summary information about the sections and appendices that comprise the *Microsoft SQL Server Database Security Checklist V8R1.2,* and defines its scope. Supporting documents consulted are listed in this section.
Section 2	SRR Result Report
	This section is the matrix that provides a table list for the reviewer to manually document review results of the SRR process for Microsoft (MS) SQL Server.
Section 3	Checklist Procedures
	This section includes instruction to the reviewer on how to proceed with the conduct of the Microsoft SQL Server security review. It includes a list of interfaces and tools required to complete the review.
Section 4	SQL Server Check Procedures
	This section includes the procedures to determine the final finding result for each check against the SQL Server.
Appendix A	Information Assurance Vulnerability Management (IAVM) Bulletin Compliance
	IAVM's issued against the SQL Server are assigned to the host platform. This section provides this information.
Appendix B	Record of Changes
	This appendix summarizes the changes made to this document.
Appendix C	VMS SQL Server SRR Process Guide for Databases
	This appendix provides instructions for entering SRR results into VMS.
Appendix D	STIG STIGID / Checklist Discrepancy List
	This appendix provides a list of STIG requirements that are not associated with requirements in this checklist. A disposition of each requirement is provided.

1.3 Supported Versions

This checklist provides instructions for review of MS SQL Server 7, MS SQL Server 2000 (AKA version 8) and MS SQL Server 2005 (AKA version 9).

1.4 Document Effective Date

This document is current as of the release date. Updates are made to update underlying DOD policy or to correct errors, omissions, or to clarify guidance.

1.5 Review Method

The goal is to perform a successful Security Readiness Review (SRR) of SQL Server. An SRR evaluation script that measures compliance for some check items listed in this document is available. These checks are:

1. **Interview** – The information required to complete this check is obtained through interviews and reviews of documentation
2. **Manual** – The information required to complete this check may lie in both system settings and via review of documentation
3. **Verify** – The information required to complete the check can usually be obtained programmatically, but must be verified for accuracy
4. **Auto** – The information required to complete the check can be obtained programmatically and is reliably accurate.

1.6 Referenced Documents

The following table enumerates the documents and resources consulted:

Date	Document Description
19 Sep 2007	*Database Security Technical Implementation Guide, Version 8, Release 1*
6 Apr 2007	*Benchmark for SQL Server 2005 Version 1.0, The Center for Internet Security*
2007	*Microsoft SQL Server 2005 Books Online*
2007	*Microsoft SQL Server 2000 Books Online*
2000	*Microsoft SQL Server 7 Books Online*

2. SQL Server SRR Results Report

Unclassified UNTIL FILLED IN
CIRCLE ONE
FOR OFFICIAL USE ONLY, (mark each page)
CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:
Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

This checklist will become effective on **15 Jun 2008**.

Reviewer:		Date:	
System:		Type of Review (Remote, Sample, Full):_____	

Finding Totals: **Comments:**

Category I: _____
Category II: _____
Category III: _____

Total:

2.1 Site Information

Site:			
System Administrator Information:			
Name:			
E-mail Address:			
Phone # (Commercial):	( )	DSN:	
IAO Information:			
Name:			
E-Mail Address			
Phone # (Commercial)	( )	DSN:	
DBA Information:			
Name:			
E-mail Address:			
Phone # (Commercial):	( )	DSN:	

2.2 System Information

System Detail	
System ID or Host Name	
Hardware Platform	
Operating System	
Operating System Version	
Relational Database Management System	
Relational Database Management System Version	
RDBMS Software OS Owner Account Name	
Database Instance Identifier	
COTS/GOTS Application / Schema Name(s)	
Application Software OS Owner Account Name	
Instance IP Port Listening on	
Number/Name of Other Instances/RDBMS on this Host	

Summary of Database SRR Findings By Category		
Category	**Total Possible Findings**	**Actual Findings**
Category I	9	
Category II	162	
Category III	20	
Total Findings	191	

2.3 SRR Results

(Method: Auto=Automated by script, Verify = Script returns information to complete review, Manual = Script does not provide data. Results determined by following technical procedure; Interview = Results determined by examining documentation and interviewing responsible personnel (usually IAO or DBA)).

Listed in order of Method, Instance/DB, Method, STIGID / VMSKEY

3. SQL Server Security Review Procedures

3.1 Review Process Notes

A security review of Microsoft SQL Server may be completed entirely by following the procedures in this section. Each security compliance item of interest is listed with procedures for determining whether the current SQL Server installation is configured to be compliant with the requirement or not. Each security item procedure is referred to as a "check". A security item is also referred to as "vulnerability".

There may be more than one installation of SQL Server software on a single host platform. There may be multiple SQL Server Database engines defined per SQL Server software installation.

An automated script is available to assist in the SQL Server security compliance review process. Where available for use, the script may provide complete or partial determination of compliance for some checks as described below.

The checks are categorized into the following two categories and four types:

Categories:

- **Installation Checks** – These checks are applicable once per each SQL Server software installation. Some of these checks refer to the Microsoft network communication configuration and services which in most cases occur only once per database host server.
- **SQL Server Database Checks** – These checks are applicable once per each SQL Server Database. Each SQL Server Database must be checked, as there are significant security configurations that can be exploited per database.

Types:

- **Automated checks** – The SQL Server SRR script provides a complete result for the vulnerability.
- **Verify checks** – The SQL Server SRR script provides data to aid the reviewer in completing the result determination. The reviewer need only verify the data returned by the script to determine the final compliance status.
- **Manual checks** – The SQL Server SRR script provides no data or results for the check. The reviewer must complete the technical procedure in its entirety to determine the compliance status.
- **Interview checks** – The SQL Server SRR script provides no data or results for the check. The check procedures require a review of available documentation and interviews of the IAO, DBA or other database point-of-contact to determine the compliance status.

The SQL Server SRR evaluation script is available from the http://iase.disa.mil web site. The script is limited to assessing compliance with security requirements that are

configuration items on either the host operating system or the SQL Server Database or installation itself.

The purpose of this separation of checks by installation and database is to ensure that all multiple occurrences of security controls are reviewed individually and to avoid duplication of control reviews that affect multiple other security levels. The additional separations are meant to assist the reviewer to complete the review more efficiently by grouping checks together that are completed using the same method or tool such as referring to the documentation in the System Security Plan or using SQL Server 7 & 2000 **osql** command line utility or SQL Server 2005 **sqlcmd** command line utility to review settings. Therefore, a complete review of SQL Server includes one status for each installation check and one status of each database check *per defined database*. SQL Server begins with a default of four (4) databases so four results for each database level check would be required.

3.2 IAVM Compliance

Security patches required by the DOD IAVM process are reviewed during an operating system security review. Information for security patch compliance for SQL Server is available in Appendix A of this SQL Server Database Security Checklist.

3.3 Review Tools and Interfaces

Run the review procedures and utilities listed below from the Windows SQL Server host system.

The procedures assume a familiarity with use of the following Windows tools:

- Windows Explorer – Review file directory permissions and disk partition information
- Windows Registry Editor – Review registry values and permissions
- Windows Microsoft Management Console (MMC) – Review various Windows items including users, groups, and services

The procedures also assume a familiarity with the SQL Server Transact-SQL (TSQL) language and the following SQL Server tools:

- SQL Server Enterprise Manager (7 & 2000)
- SQL Server Management Studio (2005 & 2008)
- SQL Server Configuration Manager
- SQL Server Network Utility
- SQL Server Query Analyzer
- SQL Server 2005 **sqlcmd** command line utility OR
- SQL Server 7 & 2000 **osql** command line utility or a tool of the reviewer's choice that accepts and runs TSQL commands against a SQL Server instance

The procedures provide a reference to any tool applicable to the completion of the procedure. Where the procedure begins with the text:

From the query prompt:

The TSQL command that follows this text is to be run from the SQL Server command line tool osql or sqlcmd, Query Analyzer, or the TSQL command tool of the reviewer's preference. Where required by the tool, it may be necessary to follow commands with the "GO" command to engage the tool to process the command entered. This is the case with **osql**. The SQL Server Query Analyzer requires only the selection of the Execute function to process the command.

Included in the script package is a "ChecktoText" file in html format that has all of the check text. This is to allow a simple cut-and-paste of the query commands by the reviewer to the query prompt or window. There are differences between the manual check query text from the script that allows individual checks to be run outside of programming structures and without storage of results in temporary tables.

This document does not provide instruction for use of any tools referenced. Please refer to vendor documentation for access to and use of the required vendor tools. Instructions for use of the SQL Server SRR script are included with the script and not provided in this document.

3.4 System Security Plan Overview

Some procedures within this checklist refer to the System Security Plan (SSP). The System Security Plan is referenced in the DOD Instruction 8500.2 in the following IA control as:

DCSD-1 IA Documentation

All appointments to required IA roles (e.g., DAA and IAM/IAO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance and IT-designation. A System Security Plan is established that describes the technical, administrative and procedural IA program and policies that govern the DOD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup or emergency response).

A template for creating an SSP may be found on the DIACAP Knowledge Service (https://diacap.iaportal.navy.mil/), DIACAP Resources, DIACAP Reference Library, Sample Documents, *ISP_Sample.doc (zipped)* or the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-18, *Guide for Developing Security Plans for Federal Information Systems*. This document may be found at http://csrc.nist.gov/publications/PubsSPs.html. The DIACAP Knowledge Service also provides a matrix of documentation requirements for the IA Controls to those required under the previous DITSCAP System Security Authorization Agreement

(SSAA). The matrix may be found under IA Controls, Information on the IA Controls Matrix of IA Controls to Documentation.

Information required and verified by the procedures in this checklist should be contained in the SSP under the IA control referenced. However, this document concerns itself only with the specific controls referenced in it and does not review and verify the entirety of the SSP.

3.5 Automated Information System (AIS) Functional Architecture Document

The DODI 8500.2 defines an AIS functional architecture document under IA control DCFA as:

DCFA-1 Functional Architecture for AIS Applications

For AIS applications, a functional architecture that identifies the following has been developed and is maintained:

- All external interfaces, the information being exchanged, and the protection mechanisms associated with each interface - user roles required for access control and the access privileges assigned to each role (See ECAN)
- Unique security requirements (e.g., encryption of key data elements at rest)
- Categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA)
- Restoration priority of subsystems, processes, or information (See COEF)

Additional information may be obtained for this IA control from the DIACAP Knowledge Service.

3.6 Sensitive Data Protection and Definition

Databases, as frequent repositories for sensitive data, are often relied upon for providing an additional layer of protection for such data. The responsibility for determining what protections should be employed for sensitive data falls to the Information Owner as the person that best understands the purpose, function, and the possible impact of unauthorized release of the data. Most commonly, authentication and authorizations are sufficient to protect data against unauthorized release. However, in some cases encryption may be used to assist in protecting against disclosure where authorizations do not provide needed restrictions. For example, the access provided to DBAs to administer the DBMS provides them with access to all data stored within the database.

The DODD 8500.1 provides the following definition for sensitive data:

Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act", but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987"). Examples of sensitive information include, but are not

limited to information in DOD payroll, finance, logistics and personnel management systems. Sensitive information sub-categories include, but are not limited to, the following:

For Official Use Only (FOUO) - In accordance with DOD 5400.7-R (reference (ab)), DOD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) Privacy Data. Any record that is contained in a system of records as defined in the Privacy Act of 1974 (5 U.S.C. 552a) (reference (z)) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

DOD Unclassified Controlled Nuclear Information (DOD UCNI) - Unclassified Information on security measures (including security plans, procedures, and equipment) for the physical protection of DOD Special Nuclear Material (SNM), equipment, or facilities in accordance with DOD Directive 5210.83. Information is Designated DOD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DOD SNM, equipment, or facilities.

Unclassified Technical Data - Data that is not classified but is subject to export control and is withheld from public disclosure according to DOD Directive 5230.25.

Proprietary Information - Information that is provided by a source or sources under the condition that it not be released to other sources.

Foreign Government Information - Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with DOD 5200.1-R.

Department of State Sensitive But Unclassified (DoS SBU) - Information that originated from the Department of State (DoS) that has been determined to be SBU under appropriate DoS information security polices.

Drug Enforcement Administration (DEA) Sensitive Information - Information that is originated by the Drug Enforcement Administration and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

3.7 Process Notes

The execution of the SQL Server SRR script and many of the manual procedures require SYSADMIN privileges in the SQL Server instance. Some operating system commands require Administrator privileges to the host operating system. This will vary based on the permissions assigned to the account used. It is recommended that the account used for installation of SQL Server be used to process the security review as this account is expected to have the required access permissions. It is expected that an authorized DBA or the IAO log and monitor this account.

3.8 Check Reference Numbering Scheme

The checks use two different reference numbers: the STIGID and VMSKEY. The STIGID is a manually assigned reference number. The database STIGID assignments including those for SQL Server begin with two letters that indicate the following:

- **DG** – This is a General database check and the fundamental requirement is required of any DBMS product where available.

- **DM** – This is a Microsoft SQL Server specific check and does not apply as written to any other DBMS products.
- **DO** – This is an Oracle specific check and does not apply as written to any other DBMS products.
- **DI** – This is an IBM DB2 specific check and does not apply as written to any other DBMS products.

Only checks of type "DG" and "DM" are included in this checklist. All "DM" checks include references to "DG" checks that help map the check to the security requirement as listed in the Database STIG.

3.9 Version Specific Checks

Any checks that are applicable to a specific version or versions of SQL Server include reference to the applicability. All checks without such a version reference apply to all versions of SQL Server listed in paragraph 1.3.

3.10 Documentation Conventions

Conventions used in this document:

- The "\" character – This character is used to separate selection items. For example, registry folders and predefined keys and key values are listed as HKLM\Software\Microsoft where HKLM represents the top registry folder HKEY_LOCAL_MACHINE, Software is a folder under HKLM, etc. In addition, Start \ All Programs means click on the Start button in the Windows task bar and then select the All Programs icon.

- The "[ ]" characters are used to indicate that a replacement value provided by the reviewer is required. For example, the query command " use '[database name]' should be replaced by the reviewer with the appropriate database name as " use 'master' ". The "[]" characters should not be included in the command.

3.11 Procedure Table Data

Information Assurance (IA) Control

Each check is derived and associated with an IA Control from the DOD Instruction 8500.2. These are listed in the enclosures for the instruction and are applicable to the DBMS based on the Mission Assurance Category (MAC) determined for the system. Where the IA breakdown based on MAC is not listed in the table in this document, the check requirement applies to all level systems or the IA control does not have

breakdowns. Where a check applies to only one IA control and MAC level, the level is specified in the table.

Policy:

Each check is assigned a Gold, Platinum or All Policies (both) designation based on implementation difficulty. Gold requirements are those whose implementation is unlikely to interrupt system operation. Platinum requirements require consideration that is more careful and testing prior to implementation. Please note that no changes to the DBMS should be made without a careful review or test of potential impact. Also, note that the Vulnerability Maintenance System (VMS) lists each "check" as being Gold, Platinum or both. In most cases where Policy = All Policies in this document, in VMS would be identified as both Gold and Platinum, with Platinum considerations to be taken into account.

Mission Assurance Category (MAC)/Confidentiality:

This field shows the applicability of the check based on the mission criticality and confidentiality of the system under review. The DODI 8500.2 defines three levels of mission criticality where a MAC level of one requires the highest level of integrity and availability protection and a level three requires the lowest. The confidentiality levels are Public, Sensitive and Classified. Please see DODI 8500.2 for more information on determining the MAC and Confidentiality for the system.

Check Type:

This indicates the method available for determining the compliance to the check. Auto indicates that the available SRR evaluation script can be used to determine compliance. Verify means that the SRR script provides information to assist in a manual determination of check compliance and in some cases may be able to determine some level of compliance such as applicability. Interview means that the check does not require any technical or system hands-on actions. Rather it requires a review of documentation and in some cases verbal confirmation by the DBA or IAO. A check type of manual indicates the check procedure requires hands-on technical review of the security configuration item that the script is unable to complete. In VMS, the checks listed as (Script) are equivalent to Check Type: Manual.

Database Level:

This indicates whether the check is performed once per defined database instance (True) or once per installation of the DBMS and DBMS Engine (False)

Documentable:

This field is used to indicate whether the check script result may be verified for pre-determined compliance automatically in the Vulnerability Management System (VMS).

VKEY:

This is the check reference number for VMS.

STIG Requirement:

This is the policy requirement as mapped from the Database STIG document. The policy requirement is a general requirement for all databases. Some configuration items specific to a particular DBMS product are more loosely associated with the general statement.

Severity:

This is the severity code assignment for this check. The severity code may sometimes differ from the severity assigned to the STIG requirement because it is has a more or less severe implication. Severity code definitions are documented in Section 1.1 – Overview in this document.

4. SQL Server Installation Check Procedures

4.1 DG0001: DBMS version support

Description: The version of MS SQL Server must be listed by Microsoft as a supported version. Microsoft discontinues fixes for unsupported versions on reported dates. In order to maintain a secure environment, the installed version must continue to receive fixes for reported vulnerabilities.

Check:

From the SQL Server Enterprise Manager or SQL Server Management Studio GUI:

Right-click on SQL server name, select General tab or pate, review Product Version or Version.

OR

From the query prompt:

```
SELECT CONVERT(CHAR(13), SERVERPROPERTY('ProductVersion'))
```

Where format is in *major.minor.build* and we only concern ourselves with the major version:

7 = SQL Server 7
8 = SQL Server 2000
9 = SQL Server 2005
10 = SQL Server 2008

If the major version listed is not under Mainstream or Extended support from Microsoft as listed in the table below, this is a Finding.

You can verify support for SQL Server at the following website:

http://support.microsoft.com/gp/lifepolicy

Product Release	Mainstream Support Retired	Extended Support Retired
SQL Server 7	12/31/2005	01/11/2011
SQL Server 8 (2000)	04/08/2008	04/09/2013
SQL Server 9 (2005)	04/12/2011	04/12/2016
SQL Server 10 (2008)	01/14/2014	01/08/2019

The reviewer may want to record the version number for other checks in this review. Service patch level and HOTFIX updates are reviewed in separate checks. IAVM compliance is reviewed in Windows OS checks.

Fix:

Protect the SQL Server installation from published vulnerabilities by upgrading to a supported version and installing all service packs and HOTFIXes as they become available (after testing).

VKEY: V0005658	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: VIVM	Check Type: Auto	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.6.1			
STIG Requirement:	(DG0001: CAT I) The IAO will ensure unsupported DBMS software is removed or upgraded prior to a vendor dropping support.			

4.2 DG0002: DBMS version upgrade plan

Description: Unsupported software versions are not patched by vendors to address newly discovered security versions. An unpatched version is vulnerable to attack. Developing and implementing an upgrade plan prior to a lapse in support helps to protect against published vulnerabilities.

Check:

If the check for unsupported version (DG0001) returns an unsupported version or the installed version is within 6 mos. of a desupport notice, ask if migration plans are in progress to upgrade to a supported version. If plans are not in progress, this is a Finding.

To check version for SQL Server:

From the query prompt:

```
SELECT CONVERT(CHAR(13), SERVERPROPERTY('ProductVersion'))
```

Where format is in *major.minor.build* and we only concern ourselves with the major version:

7 = SQL Server 7
8 = SQL Server 2000
9 = SQL Server 2005
10 = SQL Server 2008

From the query prompt:

```
SELECT CONVERT(CHAR(3), SERVERPROPERTY('ProductLevel'))
```

Where value:

RTM = Original release version (no service packs installed)
SPn = Service Pack Level

View version and service pack level. If the DBMS is not at the service pack level listed for the version below and no update plan exists, this is a Finding.

If the SQL Server version is version 7 or version 8, review evidence that Microsoft Extended Support has been purchased to continue support.

If Extended Support has not been purchased, this is a Finding.

If Extended Support will expire within 6 months, ask the IAO to provide evidence that an upgrade to a supported version or an extension to the support is planned and in progress. If it is not, this is a Finding.

Product Release (as of 1 May 2009)	Mainstream Support Retired	Extended Support Retired	Service Pack
SQL Server 7	12/31/2005	01/11/2011	SP4
SQL Server 8 (2000)	04/08/2008	04/09/2013	SP4
SQL Server 9 (2005)	04/12/2011	04/12/2016	SP3
SQL Server 10 (2008)	01/14/2014	01/08/2019	SP1

Fix:

Apply the latest service pack (after testing) for the supported DBMS version. Create an upgrade plan for obsolete or expiring vendor products. As soon as an expiration date is published for the product, prepare to upgrade it. The cost of the upgrade should be budgeted including any additional testing and development required supporting the upgrade.

A plan for testing the upgrade should also be scheduled. Any other steps for upgrade should be included in the plan and the plan for upgrade should be scheduled for completion prior to expiration of the current product or product support contract.

VKEY: V0004758	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: VIVM	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.6.1			
STIG Requirement:	(DG0002: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading DBMS systems 6 months prior to the date the vendor drops security patch support.			

4.3 DG0003: DBMS security patch level

Description: Maintaining the currency of the software version protects the database from known vulnerabilities.

Check:

From the query prompt:

SELECT CONVERT(CHAR(13), SERVERPROPERTY('ProductVersion'))

Where format is in *major.minor.build*

From the query prompt:

SELECT CONVERT(CHAR(3), SERVERPROPERTY('ProductLevel'))

Where value:

RTM = Original release version (no service packs installed)
SPn = Service Pack Level

Note: HOTFIXes are generated and applied to specific Service Packs and are reflected in the Product Version build segment as an incremental version.

Product Release	Service Pack	Product Version
SQL Server 7	SP4	7.00.1063
SQL Server 8 (2000)	SP4 + HOTFIX	8.00.2187
SQL Server 9 (2005)	SP3	9.00.4035
SQL Server 10 (2008)	SP1	10.00.2531

For any product listed above, if the Product Version is the same or numerically higher than what is listed above, this is Not a Finding. If the Product Version is numerically lower, this is a Finding.

Note: If any update has been released that is deemed by Microsoft to be a critical update, this check should be assigned a Severity Category of I.

Supported versions and Service Packs are listed on the Microsoft web sites:

http://support.microsoft.com/gp/lifeselectserv
http://support.microsoft.com/kb/321185/en-us (lists version numbers)

Fix:

Upgrade to the latest SQL Server Service Pack. Apply all applicable Microsoft SQL Server critical updates and HOTFIXes.

VKEY: V0005659	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: VIVM	Check Type: Auto	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.6.1			
STIG Requirement:	(DG0003: CAT II) The DBA will ensure all applicable vendor-provided security patches are installed.			

4.4 DG0005: DBMS administration OS accounts

Description: Database administration accounts are frequently granted more permissions to the local host system than are necessary. This allows inadvertent or malicious changes to the host operating system.

Check:

Review host system privileges assigned to the DBA accounts. If any are granted host system administrator privileges or other system privileges not required for DBMS administration, this is a Finding.

The DBA should have only the OS Users group, custom SQLServer DBA group, SQL Server service groups and custom SQL Server Users groups assigned. The custom SQL Server groups should have only the Log on Locally user right assigned.

Fix:

Revoke any host system privileges from DBA accounts not required DBMS administration.

Revoke any OS group memberships that assign excess privileges to DBA accounts.

Remove any directly applied permissions or user rights from the DBA account.

VKEY: V0006756	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: SA/DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0005: CAT II) The SA/DBA will ensure database administration OS accounts required for operation and maintenance of the DBMS are assigned the minimum OS privileges required by the specific DBMS to perform DBA functions.			

4.5 DG0009: DBMS software library permissions

Description: The DBMS software libraries contain the executables used by the DBMS to operate. Unauthorized access to the libraries can result in malicious alteration or planting of operational executables. This may in turn jeopardize data stored in the DBMS and/or operation of the host system.

Check:

Check access to SQL Server program files and directories:

For SQL Server 7 & 2000:

The default SQL Server instance software directory is where [drive] is selected during install:

[drive] \Program Files\Microsoft SQL Server\

The default SQL Server instance data directory is:

[drive] \Program Files\Microsoft SQL Server\MSSQL\Data

The directory under which the SQL Server instance is installed is listed in the registry under:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ Setup \ SQLPath

The default instance name is MSSQLServer. Instance names are listed in the registry under:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ InstalledInstances

The default directory for storage of SQL Server data files is listed in the registry under:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ [instance name] \ MSSQLServer \ DefaultData

File permissions may be reviewed individually using Windows explorer by navigating to the directory specified and viewing the Security properties. There are also tools available that are designed to streamline review of file permissions.

Verify that the permissions are equal to or more restrictive than the following:

Non-Executable Files = Read
Executable Files = Read, Execute
Folders = Read, Execute, List Folder Contents

The following groups may have Full Control assigned to any or all identified directories or files:

1. Administrators (builtin group)
2. DBAs (custom group)
3. CREATOR OWNER (builtin)
4. SYSTEM (builtin)
5. SQL Server Service Account

The SQL Server Service Account name is in the registry listed under:

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ MSSQL [instance name] \ ObjectName

If permission assignments are less restrictive than listed, this is a Finding.

If permission assignments are granted to the Builtin USERS group, this is a Finding.

For SQL Server 2005:

SQL Server program files are installed in two places:

1. A subdirectory of Program Files directory named Microsoft SQL Server (specified here as [PFdir])
2. The directory created for the specific instance (specified here as [InstDir]).

This directory is specified in the registry for database engine instances under:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ Instance Names \ SQL

Instances for Reporting Services and Analysis Services are listed under the registry keys:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ Instance Names \ RS

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ Instance Names \ OLAP

File permissions may be reviewed individually using Windows explorer by navigating to the directory specified and viewing the Security properties. There are also tools available that are designed to streamline review of file permissions.

Verify that the permissions are equal to or more restrictive than listed below:

The following groups may have Full Control assigned to any or all [PFdir] or [InstDir] directories or files:

1. Administrators (builtin group)
2. DBAs (custom group)
3. CREATOR OWNER (builtin)
4. SYSTEM (builtin)
5. SQL Server Service Account

The following directories should be restricted to other accounts or groups as listed below:

Directory/file | Account or Group | Permissions

[PFdir]\80\tools | SQL Services Users | Read, Execute
[PFdir]\90\com | MSSQLServer, SQLServerAgent | Read, Execute
[PFdir]\90\dts | SQL Services Users | Read, Execute
[PFdir]\90\dts\binn | MSDTSServer | Read, Execute
[PFdir]\90\dts\binn\MsDtsSrvr.ini.xml | MSDTSServer | Read
[PFdir]\90\Notification services | Notification services | Read, Execute, list folder contents
[PFdir]\90\sdk | SQL Services Users | Read
[PFdir]\90\shared | MSSQLServer, SQLServerAgent, FTS MSSQLServerOLAPservice, SQLServer2005ReportServerUser, SQLServer2005ReportingServicesWebServiceUser, Notification Services, MSDTSServer, SQL Server Browser | Read, Execute
[PFdir]\90\shared\Errordumps | MSSQLServer, SQLServerAgent, FTS MSSQLServerOLAPservice, SQLServer2005ReportServerUser, SQLServer2005ReportingServicesWebServiceUser, Notification Services, MSDTSServer, SQL Server Browser | Read, Write
[PFdir]\90\shared\msmdlocal.ini | MSSQLServerOLAPservice | Full control
[PFdir]\90\shared\msmdlocal.ini | SQL Server Browser | Read
[PFdir]\90\tools | SQL Services Users | Read, Execute
[PFdir]\90\Setup Bootstrap | SQL Services Users | Read, Execute
[InstDir]\MSSQL\backup | MSSQLServer, SQLServerAgent | Full control
[InstDir]\MSSQL\binn | SQL Services Users | Read, Execute
[InstDir]\MSSQL\data | MSSQLServer | Full control
[InstDir]\MSSQL\FTData | MSSQLServer, FTS | Full control
[InstDir]\MSSQL\FTRef | FTS | Read, Execute

[InstDir]\MSSQL\Install | MSSQLServer, FTS | Read, Execute
[InstDir]\MSSQL\jobs | SQLServerAgent | Full control
[InstDir]\MSSQL\Log (all files) | MSSQLServer, SQLServerAgent | Full control
[InstDir]\MSSQL\Log\(all files except .trc files) | FTS | Full control
[InstDir]\MSSQL\Repldata | MSSQLServer | Full control
[InstDir]\MSSQL\Template Data (SQL Server Express Only) | MSSQLServer | Read
[InstDir]\OLAP | MSSQLServerOLAPservice | Read, Execute
[InstDir]\OLAP\Backup | MSSQLServerOLAPservice | Full control
[InstDir]\OLAP\Config | MSSQLServerOLAPservice | Full control
[InstDir]\OLAP\Data | MSSQLServerOLAPservice | Full control
[InstDir]\OLAP\Log | MSSQLServerOLAPservice | Read, Write
[InstDir]\Reporting Services\Log Files | SQLServer2005ReportServerUser, SQLServer2005ReportingServicesWebServiceUser | Read, Write, Delete
[InstDir]\Reporting Services\ReportManager | SQLServer2005ReportServerUser, SQLServer2005ReportingServicesWebServiceUser, SQL Services Users | Read, Execute
[InstDir]\Reporting Services\ReportManager\pages | SQLServer2005ReportingServicesWebServiceUser, SQL Services Users | Read
[InstDir]\Reporting Services\ReportManager\Styles | SQLServer2005ReportingServicesWebServiceUser, SQL Services Users | Read
[InstDir]\Reporting Services\ReportManager\webctrl_client\1_0 | SQLServer2005ReportingServicesWebServiceUser | Read
[InstDir]\Reporting Services\ReportServer | SQLServer2005ReportServerUser, SQLServer2005ReportingServicesWebServiceUser, SQL Services Users | Read, Execute
[InstDir]\Reporting Services\reportservice.asmx | SQLServer2005ReportingServicesWebServiceUser, SQL Services Users | Full Control
[InstDir]\Reporting Services\RSTempfiles | SQLServer2005ReportServerUser, SQLServer2005ReportingServicesWebServiceUser | Read, Write
[InstDir]\ReportingServices\ReportServer\global.asax | SQLServer2005ReportServerUser, SQLServer2005ReportingServicesWebServiceUser | Full control
[InstDir]\ReportingServices\ReportServer\global.asax | SQL Services Users | Read
[InstDir]\ReportingServices\ReportServer\ReportServer.config | SQLServer2005ReportServerUser, SQLServer2005ReportingServicesWebServiceUser | Read, Write
[InstDir]\MSSQL\binn | Performance Log Users, Performance Monitor Users | List folder contents

[InstDir]\MSSQL\binn\sqlctr90.dll | Performance Log Users, Performance Monitor Users | Read, Execute

If permission assignments are less restrictive than listed, this is a Finding.

If permission assignments are granted to the Builtin USERS group, this is a Finding.

Fix:

Restrict access to SQL Server files and directories as directed in the check.

VKEY: V0015608	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSL	Check Type: Manual	Database Level: False	Responsibility: SA/DBA	Documentable: False
Reference:	Database STIG 3.1.10			
STIG Requirement:	(DG0009: CAT II) The SA/DBA will ensure access to DBMS software is restricted to authorized OS accounts.			

4.6 DG0010: DBMS software monitoring

Description: Changes to files in the DBMS software directory including executable, configuration, script or batch files can indicate malicious compromise of the software files. Changes to non-executable files, such as log files and data files, do not usually reflect unauthorized changes but are modified by the DBMS as part of normal operation. These modifications can be ignored.

Check:

Ask the DBA to describe/demonstrate any software modification detection procedures in place and request documents of these procedures to review. If procedures exist that include review of the database software directories and database application directories, this is Not a Finding. Verify by reviewing reports for inclusion of the DBMS executable and configuration files:

Sample Questions: What procedures/software do you have in place to detect unauthorized modification to application files? Are the database application software files including both the SQL Server and third party files scanned for modification? Do you scan for modifications to the configuration files?

Fix:

Establish and implement procedures to monitor any changes made to the database software. Identify all database files and directories to be included in the host system or database backups and provide these to the person responsible for backups.

For Windows systems, use the **dir /s > filename.txt** run weekly to store and compare file modification/creation dates and file sizes using the DOS fc command. This is not as comprehensive as some tools available, but may be enhanced by also checking checksum or file hashes.

VKEY: V0002420	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSL	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.10			
STIG Requirement:	(DG0010: CAT III) The IAO will ensure DBMS software is monitored on a regular basis no less frequently than weekly to detect unauthorized modifications.			

4.7 DG0011: DBMS Configuration Management

Description: Uncontrolled, untested or unmanaged changes result in an unreliable security posture. All software libraries related to the database and its used need to be reviewed, considered, and the responsibility for Configuration Management (CM) assigned. CM responsibilities may appear to cross boundaries of responsibility. It is important, however, for the boundaries of CM responsibility to be clearly defined and assigned to ensure no libraries or configurations are left unaddressed. Related database application libraries may include third-party DBMS management tools, DBMS stored procedures, or other end-user applications.

Check:

If this is not a production system, this check is Not Applicable.

Interview the DBA to ask if configuration management procedures are in place to prevent untested and uncontrolled software modifications to the production system. If none is in place, this is a Finding.

Sample questions: What procedures do you follow to introduce new software to the production system? Are the modifications tested prior to installation on the production system?

Fix:

Develop and implement configuration management procedures. Include all configurable DBMS features or options. Include upgrades and patch management. Assign responsibilities for oversight and approval for all changes to the database software and configuration.

VKEY: V0003726	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCPR/DCCB	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.8			
STIG Requirement:	(DG0011: CAT III) The IAO will ensure configuration management procedures are documented and implemented for changes to the DBMS configuration, software libraries and other related application software libraries.			

4.8 DG0012: DBMS software storage location

Description: Multiple applications can provide a cumulative negative effect on the overall system security posture. A vulnerability and subsequent exploit to one application can lead to an exploit of other applications sharing the same security context. For example, an exploit to a web server process that leads to unauthorized administrative access to the host system can most likely lead to a compromise of all applications hosted by the same system. A DBMS not installed on a dedicated host both threatens and threatened by other hosted applications. Applications that share a single DBMS may also create risk to one another. Access controls defined for one application may provide by default access to the other application's database objects or directories. Any method that provides any level of separation of security context assists in the protection between applications.

Check:

Review the SQL Server software library directory. The SQL Server software library is defined in the registry key:

For SQL Server 7 & 2000:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ MSSQLServer \ Setup \ SQLPath

For SQL Server 2005:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ Setup \ SQLProgramDir

Note any custom subdirectories within the SQL Server software library directory.

If any directories or files not installed with the SQL Server software exist with the SQL Server software directory, this is a Finding.

Only applications that are required for the functioning and administration, not use, of the DBMS should be located on the same disk partition as the DBMS software libraries.

Fix:

Install all applications on partitions or directories separate from the SQL Server software library directory. Re-locate any directories or re-install other application software that currently shares the DBMS software library directory to separate disk partitions or directories.

VKEY: V0004754	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP
IA Control: DCPA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.6			
STIG Requirement:	(DG0012: CAT II) The DBA will install and maintain database software directories including DBMS configuration files in dedicated directories or disk partitions separate from the host OS and other applications.			

4.9 DG0013: Database backup procedures

Description: Database backups provide the required means to restore databases after compromise or loss. Backups help reduce the vulnerability to unauthorized access or hardware loss.

Check:

Review the database backup procedures and implementation evidence. Evidence of implementation includes records of backup events and physical review of backup media. Evidence should match the backup plan as recorded in the System Security Plan.

If backup procedures do not exist or not implemented in accordance with the procedures, this is a Finding.

If backups are not performed weekly or more often for MAC III systems, this is a Finding

If backups are not performed daily or more often for MAC II systems, this is a Finding

If backup data for MAC II systems is not secured and stored offline at an alternate site, this is a Finding.

If backups for MAC 1 systems do not include a redundant secondary system maintained at a separate physical site that can be activated without interruption or loss of data if the primary system fails, this is a Finding.

Fix:

Design and implement database backup procedures.

Include daily backup procedures and offline backup data storage at an alternate site for MAC II systems.

Include a secondary server installed at a separate location (IAW COOP guidelines) that can be brought online to prevent any disruption to availability or loss of data for MAC I systems.

VKEY: V0015126	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: CODB	Check Type: Interview	Database Level: False	Responsibility: SA/DBA	Documentable: False
Reference:	Database STIG 3.5.2			
STIG Requirement:	(DG0013: CAT II) The DBA/SA will ensure backups of database data, configuration, and other files critical to database operation have been performed at intervals consistent with the database's assigned criticality level.			

4.10 DG0014: DBMS demonstration and sample databases

Description: Demonstration and sample database objects and applications present publicly known attack points for malicious users. These demonstration and sample objects are meant to provide simple examples of coding specific functions and are not developed to prevent vulnerabilities from being introduced to the DBMS and host system.

Check:

Review the list of databases defined for the instance:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name FROM [master].dbo.sysdatabases
WHERE name IN
('Northwind', 'pubs', 'AdventureWorks', 'AdventureWorksDW',
 'AdventureWorksAS', 'DataEncryptDemo')
```

For SQL Server 2005:

From the query prompt:

```
SELECT name FROM [master].sys.databases
WHERE name IN
('Northwind', 'pubs', 'AdventureWorks', 'AdventureWorksDW',
 'AdventureWorksAS', 'DataEncryptDemo')
```

If any results are displayed, this is a Finding.

Fix:

Drop sample or demonstration databases from production instances. Verify that no production objects have been stored in the sample database prior to dropping.

```
DROP DATABASE [database name]
```

VKEY: V0015609	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Auto	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0014: CAT II) The DBA will ensure database applications, user accounts, and objects installed for demonstration of database features, experimentation, or other non-production support purposes have been removed from the database and host system.			

4.11 DG0016: DBMS unused components

Description: Unused, unnecessary DBMS components increase the attack vector for the DBMS by introducing additional targets for attack. By minimizing the services and applications installed on the system, the number of potential vulnerabilities is reduced.

Check:

Review the list of components or optional features installed with the database.

This may be most clearly displayed using the DBMS product installation tool, but may require review of the product installation documentation.

If no optional features or components are installed, this is Not a Finding.

If optional components or features are installed, then review the System Security Plan to verify that they are documented and authorized.

If any are not documented and authorized, this is a Finding.

Fix:

Review the list of optional features or components available for the DBMS product.

If any are required for operation of applications that will be accessing the DBMS, then include them in the application design specification and list them in the System Security Plan.

If any are not, but have been installed, then uninstall them and remove any database objects and applications that are installed to support them.

VKEY: V0003728	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0016: CAT III) The DBA will ensure unused optional database components or features, applications, and objects are removed from the database and host system. If the optional component cannot be uninstalled or removed, then the DBA will ensure the unused component or feature is disabled.			

4.12 DG0017: DBMS shared production/development use

Description: On shared production and development DBMS systems access identifiers that do not clearly indicate whether the DBMS or DBMS object being accessed is part of the production or development objects can lead to unintentional modification of production objects.

Check:

If the DBMS host is not a shared development/production system, this check is Not Applicable.

Review any environment variables or other identifiers configured on the host system used by both production DBAs and other users and developers to access the production and development DBMSs. If the names or values of any identifiers do not clearly distinguish the development from the production applications, databases or database objects, this is a Finding.

An example of poor identifier naming would be MYDBAPP1 for production and MYDBAPP2 for development. Acceptable identifiers would be MYDBAPP-PROD and MYDBAPP-DEV or completely different names such as FREDSAPP and SALLYSAPP where the related SALLYSAPP identifiers are known only to DBAs and Developers.

Check Windows service names and Unix process names to review identifiers as well as environment variables used by DBAs and developers. Have the DBA display any other system level or local environment variables that reference the database installation directories or instances.

Fix:

Rename identifiers or configuration parameters clearly to distinguish production applications, databases and objects from development.

VKEY: V0003803	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECSD	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.20			
STIG Requirement:	(DG0017: CAT II) The DBA will ensure software development on a production system is separated through the use of separate and uniquely identified data and application file storage partitions and processes/services.			

4.13 DG0019: DBMS software ownership

Description: File and directory ownership imparts full privileges to the owner. These privileges should be restricted to a single, dedicated account to preserve proper chains of ownership and privilege assignment management.

Check:

Review the ownership of all DBMS and dependent application software and configuration files. If the owner is other than the software installation account or the designated owner account for the file, this is a Finding.

Some configuration and log files may be owned by a service or process account. Ownership of these files should be recorded and verified accordingly.

Fix:

Assign DBMS file and directory ownership to the software installation and maintenance account.

Use the software owner account to install and maintain the DBMS software libraries and configuration files.

VKEY: V0003805	Severity: CAT 3		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSL	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.10			
STIG Requirement:	(DG0019: CAT III) The DBA will ensure database application software is owned by the authorized application owner account.			

4.14 DG0020: DBMS backup and recovery testing

Description: Problems with backup procedures or backup media may not be discovered until after a recovery is needed. Testing and verification of procedures provides the opportunity to discover oversights, conflicts or other issues in the backup procedures and media use between production and failover DBMS systems.

Check:

Review the testing and verification procedures documented in the System Security Plan.

Review evidence of implementation of testing and verification procedures by reviewing logs from backup and recovery implementation. Logs may be in electronic or hardcopy and may include email or other notification.

If testing and verification of backup and recovery procedures are not documented in the System Security Plan, this is a Finding.

If evidence of testing and verification of backup and recovery procedures does not exist, this is a Finding.

Fix:

Design, develop and implement testing and verification procedures for database backup and recovery. Include requirements for documenting database backup and recovery testing and verification activities in the procedures.

VKEY: V0015129	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: CODP	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.5.3			
STIG Requirement:	(DG0020: CAT II) The DBA will ensure the DBMS backup and recovery strategy is documented, implemented and tested at least semi-annually.			

4.15 DG0021: DBMS software and configuration baseline

Description: Without maintenance of a baseline of current DBMS application software, monitoring for changes cannot be complete and unauthorized changes to the software can go undetected. Changes to the DBMS executables could be the result of intentional or unintentional actions.

Check:

Have the DBA and/or IAO provide the DBMS software baseline procedures, implementation evidence, and a list of files and directories included in the baseline procedure for completeness.

If baseline procedures do not exist, not implemented reliably or not complete, this is a Finding.

For SQL Server 7 & 2000:

Software and configuration directories are under:

[drive] \Program Files\Microsoft SQL Server

The exact directory is specified in registry key:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ MSSQLServer \ Setup \ SQLPath

For SQL Server 2005:

Software and configuration directories are under:

[drive] \Program Files\Microsoft SQL Server

The exact directory is specified in the registry key:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Microsoft SQL Server \ 90 \ VerSpecificRootDir

For each instance, the directory and all contents specified under the registry key below where [#] is the assigned instance number:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ Setup \ SQLProgramDir

Fix:

Develop, document and implement baseline procedures that include all DBMS software files and directories. Update the baseline after new installations, upgrades or maintenance activities that include changes to the software baseline.

VKEY: V0003806	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSW	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.13			
STIG Requirement:	(DG0021: CAT II) The DBA will ensure a baseline of database application software and DBMS application objects is maintained for comparison.			

4.16 DG0025: DBMS encryption compliance

Description: Use of cryptography to provide confidentiality and non-repudiation is not effective unless strong methods are employed with its use. Many earlier encryption methods and modules have been broken and/or overtaken by increasing computing power. The NIST FIPS 140-2 cryptographic standards provide proven methods and strengths to employ cryptography effectively.

Check:

Review the DBMS documentation to determine where cryptography may be used and/or configured. If DBMS data/network encryption is not required, this check is Not a Finding.

The following product versions and editions are FIPS 140-2 certified:

SQL Server 2005 SP1, SP2 & SP3 Standard, Enterprise & Developer Editions (KB 920995)
SQL Server 2008 RTM & SP1 Standard, Enterprise & Developer Editions (KB 955720)

Review DBMS network communication encryption options, data object encryption (both tables and application code objects), and encryption key management.

Where cryptography is employed and configured by the database, review the configuration settings to see if they use:

1. Compliant algorithms (AES (128, 192 or 256), Triple DES or TDEA (3 distinct 56-bit keys), Skipjack)
2. Compliant hash functions (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-5122) 3) validated cryptographic modules (whether native to the database or not)
3. Validated cryptographic modules (whether native to the DBMS or not)

Detailed information on the FIPS 140-2 standard is available at the following website:

http://csrc.nist.gov/groups/STM/index.html

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT name, algorithm_desc FROM sys.symmetric_keys
WHERE key_algorithm NOT IN ('D3','A1','A2','A3')
ORDER BY name, algorithm_desc
```

If any records are returned, this is a Finding.

Fix:

Upgrade to a FIPS 140-2 certified SQL Server version if encryption is required by the Information Owner.

Configure cryptographic functions to use FIPS 140-2 compliant algorithms and hashing functions. If the DBMS does not employ validated cryptographic modules, consider obtaining and using a third-party FIPS 140-2 validated solution.

Note: FIPS 140-2 compliance or non-compliance for the host and network is outside the purview of the Database STIG/Checklist. FIPS 140-2 non-compliance at the host/network level does not negate this requirement.

For SQL Server 2005:

Configure symmetric keys to use approved encryption algorithms. Existing keys are not re-configurable to use different algorithms.

This may only be specified at key creation time:

```
CREATE SYMMETRIC KEY [key name] WITH ALGORITHM = AES_256
ENCRYPTION BY [certificate or asymmetric key]
```

Other approved algorithms that may be specified are TRIPLE_DES, AES_128 and AES_192.

The symmetric key must specify a certificate or asymmetric for encryption. The certificate may be the code-signing certificate used by the application.

VKEY: V0015610	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCNR	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.5			
STIG Requirement:	(DG0025: CAT II) The DBA will ensure FIPS 140-2 validated cryptography is used where encryption, digital signature, key exchange, and secure hashing is required and is configured to use NIST approved standards.			

4.17 DG0029: Database auditing

Description: Auditing provides accountability for changes made to the DBMS configuration or its objects and data. It provides a means to discover suspicious activity and unauthorized changes. Without auditing, a compromise may go undetected and without a means to determine accountability.

Check:

If C2 Auditing is enabled (See Check DM0510**:** C2 audit mode), this check is Not a Finding.

For SQL Server 2000 & 2005:

Determine the SQL Server Edition:

From the query prompt:

```
SELECT CONVERT(INT, SERVERPROPERTY('EngineEdition'))
```

If value returned is 1 (Personal or Desktop Edition) or 4 (Express Edition), if auditing is not enabled or not configured completely to requirements, review the System Security Plan. If this is properly explained in the System Security Plan, this is Not a Finding. If this is not documented or documented poorly in the System Security Plan, this is a Finding.

If value returned is 2 (Standard Edition) or 3 (Enterprise/Developer Edition), these findings apply.

Determine if trace is enabled.

For SQL Server 2000:

From the query prompt:

```
SELECT traceid 'TraceID'
FROM ::FN_TRACE_GETINFO('0')
WHERE property = 5
AND value = 1
```

For SQL Server 2005:

From the query prompt:

```
SELECT traceid 'TraceID'
FROM ::FN_TRACE_GETINFO('0')
WHERE traceid <> 1 – Do not count default trace in SQL Server 2005
```

AND property = 5
AND value = 1

If no trace is returned, this is a Finding.

If the trace returned for Check DG0145 is not returned above, this is a Finding.

Fix:

Enable the trace created in Check DG0145.

For SQL Server 2000 & 2005:

From the query prompt:

EXEC SP_TRACE_SETSTATUS [TraceID], 1

Replace [TraceID] with the ID of the trace created for the DG0145 audit trace requirement.

VKEY: V0005685	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAR	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.2			
STIG Requirement:	(DG0029: CAT II) The DBA will ensure the DBMS auditing function is enabled.			

4.18 DG0030: DBMS audit data maintenance

Description: Without preservation, a complete discovery of an attack or suspicious activity may not be determined. DBMS audit data also contributes to the complete investigation of unauthorized activity and needs to be included in audit retention plans and procedures.

Check:

Review and verify the implementation of an audit trail retention policy. Verify that audit data is maintained for a minimum of one year.

If audit data is not maintained for a minimum of one year, this is a Finding.

Fix:

Develop and implement an audit retention policy and procedure. It is recommended that the most recent thirty days of audit logs remain available online. After thirty days, the audit logs may be maintained offline. Online maintenance provides for a more timely capability and inclination to investigate suspicious activity.

VKEY: V0002507	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECRR	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.18			
STIG Requirement:	(DG0030: CAT II) The DBA will ensure the DBMS audit trail data is maintained for a minimum of one year.			

4.19 DG0031: DBMS audit of changes to data

Description: Unauthorized or malicious changes to data compromise the integrity and usefulness of the data. Auditing changes to data supports accountability and non-repudiation. Auditing changes to data may be provided by the application accessing the DBMS or may depend upon the DBMS auditing functions. When DBMS auditing is used, the DBA is responsible for ensuring the auditing configuration meets the application design requirements.

Check:

If the application does not require auditing using DBMS features, this check is Not Applicable.

Review the application System Security Plan for requirements for database configuration for auditing changes to application data.

If the application requires DBMS auditing for changes to data, review the database audit configuration against the application requirement. If the auditing does not comply with the requirement, this is a Finding.

Fix:

Configure database data auditing to comply with the requirements of the application. Document auditing requirements in the System Security Plan.

VKEY: V0015133	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-C
IA Control: ECCD	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.4			
STIG Requirement:	(DG0031: CAT II) The DBA will configure auditing of access or changes to data in accordance with the application requirements specified in the System Security Plan.			

4.20 DG0032: DBMS audit record access

Description: Audit data is frequently targeted by malicious users as it can provide a means to detect their activity. The protection of the audit trail data is of special concern and requires restrictions to allow only the auditor and DBMS backup, recovery, and maintenance users access to it.

Check:

Review the file permissions to all files located in the DBMS audit log directory. If any allow access to users not authorized as DBAs or auditors, this is a Finding.

Review database object access permissions to any audit log data stored in the database. If permissions are granted to users not authorized as DBAs or auditors, this is a Finding.

Review the file permissions to all files in the directory listed in the registry entry:

For SQL Server 7 & 2000:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ MSSQLServer \ Setup \ SQLPath \ LOG

For SQL Server 2005:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.1 \ MSSQLServer \ DefaultLog

Review permissions to the sysprotects and/or sys.dm_exec_sessions view in the Master database:

For SQL Server 7 & 2000:

```
SELECT u.name 'User', o.name 'Object', p.action 'Action'
FROM [master].dbo.sysprotects p, [master].dbo.sysobjects o,
[master].dbo.sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND o.name = 'sysprotects'
ORDER BY u.name, o.name, p.action
```

Action Codes:
26 = REFERENCES
193 = SELECT
195 = INSERT
196 = DELETE
197 = UPDATE

224 = EXECUTE

For SQL Server 2005:

```
SELECT u.name 'User', o.name 'Object', p.permission_name 'Action'
FROM [master].sys.all_objects o, [master].sys.database_principals u,
[master].sys.database_permissions p
WHERE p.grantee_principal_id = u.principal_id
AND o.object_id = p.major_id
AND (o.name = 'dm_exec_sessions' OR o.name = 'sysprotects')
ORDER BY u.name, o.name, p.permission_name
```

If any allow access to users not authorized as DBAs or auditors, this is a Finding.

Fix:

Grant audit file and database audit object access to authorized DBAs and auditors.

Revoke audit file and database audit object access from unauthorized database accounts.

VKEY: V0005686	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECTP	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.22			
STIG Requirement:	(DG0032: CAT II) The DBA will ensure DBMS audit records are protected from unauthorized access.			

4.21 DG0040: DBMS software owner account access

Description: DBA and other privileged administrative or application owner accounts are granted privileges that allow actions that can have a greater impact on database security and operation. It is especially important to grant access to privileged accounts to only those persons who are qualified and authorized to use them.

Check:

Review procedures for controlling and granting access to use of the DBMS software installation account.

If access or use of this account is not restricted to the minimum number of personnel required or unauthorized access to the account has been granted, this is a Finding.

Fix:

Develop and implement procedures to restrict use and require logging of use of the DBMS software installation account. Document authorized personnel and assignments in the System Security Plan.

VKEY: V0002422	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.11.2			
STIG Requirement:	(DG0040: CAT II) The IAO will ensure access to the DBMS software installation account is restricted to IAO-authorized personnel only.			

4.22 DG0041: DBMS installation account use logging

Description: The DBMS installation account may be used by any authorized user to perform DBMS installation or maintenance. Without logging, accountability for actions attributed to the account is lost.

Check:

Review and verify implementation of logging procedures defined for use of the DBMS software installation account. If procedures for logging access to the DBMS are not present or are not being followed, this is a Finding.

Host system audit logs should be echoed or matched in the DBMS installation account usage log along with an indication of the person who accessed the account and an explanation for the access.

Fix:

Develop and implement a logging procedure for use of the DBMS software installation account that provides accountability to individuals for any actions taken by the account.

VKEY: V0015110	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.11.12			
STIG Requirement:	(DG0041: CAT II) The IAO will ensure use of the DBMS software installation account is logged and/or audited to indicate the identity of the person who accessed the account.			

4.23 DG0042: DBMS software installation account use

Description: The DBMS software installation account is granted privileges not required for DBA or other functions. Use of accounts configured with excess privileges may result in unauthorized or unintentional compromise of the DBMS.

Check:

Review the logs for usage of the DBMS software installation account. Interview personnel authorized to access the DBMS software installation account to ask how the account is used.

If any usage of the account is to support daily operations or DBA responsibilities, this is a Finding.

Fix:

Implement policy and train authorized users to restrict usage of the DBMS software installation account for DBMS software installation, upgrade and maintenance actions only.

VKEY: V0015111	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.11.3			
STIG Requirement:	(DG0042: CAT II) The IAO will ensure the DBMS software installation account is only used when performing software installation and upgrades or other DBMS maintenance. The IAO will ensure the DBMS software installation account is not used for DBA activities not related to DBMS file permission and ownership maintenance.			

4.24 DG0050: DBMS software and configuration file monitoring

Description: Unmanaged changes that occur to the database software libraries or configuration can lead to unauthorized or compromised installations.

Check:

Review monitoring procedures and implementation evidence to verify that monitoring of changes to database software libraries, related applications and configuration files is done. Verify that the list of files, directories, and database application objects (procedures, functions and triggers) being monitored is complete.

If monitoring does not occur or is not complete, this is a Finding.

Fix:

Develop and implement procedures to monitor for unauthorized changes to DBMS software libraries, related software application libraries and configuration files.

If a third-party automated tool is not employed, an automated job that reports file information on the directories and files of interest and compares them to the baseline report for the same will meet the requirement. File hashes or checksums should be used for comparisons as file dates may be manipulated by malicious users.

VKEY: V0002423	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSL	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.10			
STIG Requirement:	(DG0050: CAT II) The DBA will ensure database application software is monitored to detect unauthorized modification every week or more often.			

4.25 DG0051: Database job/batch queue monitoring

Description: Unauthorized users may bypass security mechanisms by submitting jobs to job queues managed by the database to be run under a more privileged security context of the database or host system. These queues should be monitored regularly to detect any such unauthorized job submissions.

Check:

1. Review jobs scheduled to start automatically at system startup.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name FROM [master].dbo.sysobjects
WHERE OBJECTPROPERTY(id, 'ExecIsStartup') = 1
```

For SQL Server 2005:

From the query prompt:

```
SELECT name FROM [master].sys.procedures
WHERE is_auto_executed = 1
```

If any jobs listed are not documented as authorized, this part of the check is a Finding.

2. Review SQL Server job history

From the query prompt:

```
SELECT DISTINCT j.name
FROM [msdb].dbo.sysjobhistory h, [msdb].dbo.sysjobs j
WHERE h.job_id = j.job_id
```

If no data is listed and no jobs are listed, this part of the check is Not a Finding.

If any jobs listed are not documented as authorized, this part of the check is a Finding.

Review monitoring procedures for job queues and evidence of implementation. If procedures for monitoring job queues are not documented are not complete or are not implemented, this is a Finding.

If any part of this check results in a Finding, this is a Finding for the entire check.

Fix:

Establish and implement procedures to monitor the database job queue and job history for unauthorized job submissions. Include or note documented policy and procedures in the System Security Plan.

VKEY: V0003808	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.3			
STIG Requirement:	(DG0051: CAT II) The DBA will monitor database batch and job queues to ensure no unauthorized jobs are accessing the database.			

4.26 DG0052: DBMS software access audit

Description: Protections and privileges are designed within the database to correspond to access via authorized software. Use of unauthorized software to access the database could indicate an attempt to bypass established permissions. Reviewing the use of application software to the database can lead to discovery of unauthorized access attempts.

Check:

Review the audit trail to determine if the name of the application used to connect to the database is included. If it is not, this is a Finding.

Fix:

Modify the Audit Trail to ensure audit records include identification of the applications used to access the DBMS.

VKEY: V0003807	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAT	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.3			
STIG Requirement:	(DG0052: CAT II) The DBA will include the name of the application used to connect to the database in the audit trail.			

4.27 DG0054: DBMS software access audit review

Description: Regular and timely reviews of audit records increases the likelihood of early discovery of suspicious activity. Discovery of suspicious behavior can in turn trigger protection responses to minimize or eliminate a negative impact from malicious activity. Use of unauthorized application to access the DBMS may indicate an attempt to bypass security controls including authentication and data access or manipulation implemented by authorized applications.

Check:

Review procedures for and evidence of monitoring the audit log to detect access by unauthorized applications in the System Security Plan.

If the procedures or evidence does not exist, this is a Finding.

If alerts are not generated automatically, then manual reviews should occur weekly or more frequently. If evidence of manual reviews does not exist, this is a Finding.

Fix:

Develop, document and implement procedures for monitoring application access to the database to detect access meant to bypass security controls.

Where alerts are not implemented or available, establish weekly or more frequent review of queue activity.

VKEY: V0015611	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAT	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.3			
STIG Requirement:	(DG0054: CAT III) The IAO or Database Auditor will review the audit trail to discover access by unauthorized application software.			

4.28 DG0060: DBMS shared account authorization

Description: Group authentication does not provide individual accountability for actions taken on the DBMS or data. Whenever a single database account is used to connect to the database, a secondary authentication method that provides individual account ability is required. This scenario most frequently occurs when an externally hosted application authenticates individual users to the application and the application uses a single account to retrieve or update database information on behalf of the individual users.

Check:

Review a list of database usernames against those listed in the System Security Plan or authorized user list.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT l.name
FROM [master].dbo.sysusers u, [master].dbo.syslogins l
WHERE u.uid = l.sid
AND (l.isntuser = 1 OR l.isntname = 0)
AND l.sid <> 0x01
ORDER BY l.name
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.server_principals
WHERE type IN ('S', 'U')
AND sid <> 0x01
ORDER BY name
```

Consult the IAO or DBA to make a final determination on whether accounts listed are shared accounts.

If shared accounts are not documented and approved as shared accounts, this is a Finding.

Fix:

Use accounts assigned to individual users where feasible. Design applications to provide individual accountability (audit logs) for actions performed under a single database account. Implement other DBMS automated procedures that provide individual accountability. Where appropriate, implement manual procedures to

use manual logs and monitor entries against account usage to ensure procedures are followed.

VKEY: V0002424	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: IAGA	Check Type: Verify	Database Level: False	Responsibility: IAO/DBA	Documentable: False
Reference:	Database STIG 3.2.1			
STIG Requirement:	(DG0060: CAT II) The IAO/DBA will ensure actions by a single database account that is accessed by multiple interactive users are attributable to an individual identifier.			

4.29 DG0063: DBMS Restore Permissions

Description: Unauthorized restoration of database data, objects, or other configuration or features can result in a loss of data integrity, unauthorized configuration, or other DBMS interruption or compromise.

Check:

Review DBMS roles and accounts granted the CREATE DATABASE permission, sysadmin or dbcreator fixed server roles, and the member of each database db_owner role:

1. Accounts granted CREATE DATABASE permission or DBCREATOR server role.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.syslogins
WHERE dbcreator = 1
AND sid <> 0x01
ORDER BY name
```

For SQL Server 2005:

From the query prompt:

```
SELECT p.name 'User', r.name 'Role'
FROM [master].sys.server_principals p, [master].sys.server_principals r,
[master].sys.server_role_members m
WHERE p.principal_id = m.member_principal_id
AND r.principal_id = m.role_principal_id
AND m.role_principal_id = 9
AND m.member_principal_id <> 1
ORDER BY r.name, p.name
```

2. Accounts granted SYSADMIN permission or SYSADMIN server role.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.syslogins
WHERE sysadmin = 1
```

```
AND sid <> 0x01 ORDER BY name
```

For SQL Server 2005:

From the query prompt:

```
SELECT p.name 'User', r.name 'Role'
FROM [master].sys.server_principals p, [master].sys.server_principals r,
[master].sys.server_role_members m
WHERE p.principal_id = m.member_principal_id
AND r.principal_id = m.role_principal_id
AND m.role_principal_id = 3
AND m.member_principal_id <> 1
ORDER BY r.name, p.name
```

3. Accounts granted CREATE DATABASE permissions or granted DB_OWNER database role.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name
FROM sysprotects p, sysusers u
WHERE p.uid = u.uid
AND p.action = 203
ORDER BY u.name
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT p.name 'User', r.name 'Role'
FROM sys.database_principals p, sys.database_principals r,
sys.database_role_members m
WHERE p.principal_id = m.member_principal_id
AND r.principal_id = m.role_principal_id
AND m.role_principal_id = 16384
ORDER BY r.name, p.name
```

If any are not authorized for RESTORE permissions, this is a Finding.

The 'sa' account (SID = 0x01) and the database owner account are authorized accounts. These accounts do not require explicit authorization and do not count as a Finding.

Fix:

Define DBMS roles that are authorized for database restore functions, restrict assignment of restore privileges to those roles, and assign those roles only to authorized DBMS accounts.

VKEY: V0015107	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0063: CAT II) The DBA will restrict restore permissions on databases to DBAs and/or the database owners.			

4.30 DG0064: DBMS backup and restoration file protection

Description: Lost or compromised DBMS backup and restoration files may lead to not only the loss of data, but also the unauthorized access to sensitive data. Backup files need the same protections against unauthorized access when stored on backup media as when online and actively in use by the database system. In addition, the backup media needs to be protected against physical loss. Most DBMSs maintain online copies of critical control files to provide transparent or easy recovery from hard disk loss or other interruptions to database operation.

Check:

Review file protections assigned to online backup and restoration files.

Review access protections and procedures for offline backup and restoration files.

If backup or restoration files are subject to unauthorized access, this is a Finding.

It may be necessary to review backup and restoration procedures to determine ownership and access during all phases of backup and recovery. In addition to physical and host system protections, consider other methods including password protection to the files.

Fix:

Develop and implement protection for backup and restoration files. Document personnel and the level of access authorized for each to the backup and restoration files in the System Security Plan.

VKEY: V0015120	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: COBR	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.5.1			
STIG Requirement:	(DG0064: CAT II) The DBA will ensure access to database backup and recovery files are restricted to the database and/or OS backup and recovery processes, DBAs, and database backup/recovery operators.			

4.31 DG0065: DBMS PKI authentication

Description: In a properly configured DBMS, access controls defined for data access and DBMS management actions are assigned based on the user identity and job function. Unauthenticated or falsely authenticated access leads directly to the potential unauthorized access, misuse and lost accountability of data and activities within the DBMS. Use of PKI certificates for authentication to the DBMS provides a robust mechanism to ensure identity to authorize access to the DBMS.

Check:

If user access to the DBMS is via a portal or mid-tier system or product and PKI-authentication occurs at the portal/mid-tier, this check is Not a Finding.

Note: Privileged access to the DBMS for administration purposes is Documentable for this check. Provide a list of all accounts on the database, their purpose and steps being considered or taken to develop PKI authentication for these accounts. Implementation of PKI authentication should not be performed if doing so creates CAT I findings in any other DBMS checks.

Review the list of all DBMS accounts and their authentication methods.

This list is usually available from a system view or table and is easily gained from a simple SQL query.

If any accounts are listed with an authentication method other than a PKI certificate, this is a Finding.

Fix:

Implement PKI authentication for all accounts defined within the database where applicable.

Applications may use host system (server) certificates to authenticate.

Consider using a directory service for authentication where the DBMS does not support certificate authentication.

VKEY: V0003810	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IATS	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: True
Reference:	Database STIG 3.2.4			
STIG Requirement:	(DG0065: CAT II) The IAO will ensure a DoD PKI class 3 or 4 certificate and an approved hardware security token (DoD CAC for DoD employees or contractors) or an NSA-certified product is used for identification and authentication to the database.			

4.32 DG0066: DBMS temporary password procedures

Description: New accounts authenticated by passwords that are created without a password or with an easily guessed password are vulnerable to unauthorized access. Procedures for creating new accounts with passwords should include the required assignment of a temporary password to be modified by the user upon first use.

Check:

If all DBMS accounts are configured to authenticate using certificates or other credential besides passwords, this check is Not a Finding.

Where accounts are authenticated using passwords, review procedures and implementation evidence for creation of temporary passwords.

If the procedures or evidence do not exist or do not enforce passwords to meet DoD password requirements, this is a Finding.

Fix:

Develop and implement procedures for assigning temporary passwords to user accounts.

Procedures should include instruction to meet current DoD password length and complexity requirements and provide a secure method to relay the temporary password to the user.

Temporary passwords should also be short-lived and require immediate update by the user upon first login.

VKEY: V0003811	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2.2			
STIG Requirement:	(DG0066: CAT II) The DBA will assign a database account password at database account creation.			

4.33 DG0067: DBMS account password external storage

Description: Passwords stored in clear text for access by host applications and/or batch jobs are vulnerable to unauthorized disclosure. Passwords should always be encrypted when stored in host system files.

Check:

Review with the DBA the list of applications or batch jobs that are not defined within the database that access the database. A list of the DBMS user accounts should indicate the use of an external account as an application account (non-interactive user). Application accounts may be also be discovered by a review of available OS or DBMS batch queue entries and logs and or through a review of database audit logs.

Determine if any of the applications or batch jobs store a database password in a host system file or environment variable.

If any application accounts do access the database, ask if they store database account passwords in clear text.

If any are stored in clear text, this is a Finding.

If no list of applications and batch jobs that access the database exists, this is a Finding.

Fix:

Develop and maintain a list of batch jobs and applications that access the database and record whether they do or do not use stored credentials. Note or include list in the System Security Plan.

If passwords are stored, ensure they are encrypted and protected by host system security.

VKEY: V0003812	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2.1			
STIG Requirement:	(DG0067: CAT I) The DBA will ensure database account passwords are stored in encrypted format whether stored in database objects, external host files, environment variables or any other storage location.			

4.34 DG0068: DBMS application password display

Description: Database applications may allow for entry of the account name and password as a visible parameter of the application execution command. This practice should be prohibited and disabled, if possible, by the application. If it cannot be disabled, then users should be strictly instructed not to use this feature. Typically, the application will prompt for this information and accept it without echoing it on the users computer screen.

Check:

Interview the DBA to determine if any applications that access the database (such as sqlcmd, etc.) allow for entry of the account name and password on the command line.

If any applications exist and are in use, ask the DBA if users have been instructed not to include passwords on the command line and if these applications are monitored for compliance. If documentation of instruction and monitoring are not being performed, this is a Finding.

Fix:

Configure or modify applications to prohibit display of passwords in clear text on the command line if possible.

Implement policy and train users to prohibit entry of passwords on the command line for applications that cannot be modified or configured to deny this. Remove any applications that can access the database if they are not being used or cannot be monitored.

VKEY: V0003813	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECCR	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.5			
STIG Requirement:	(DG0068: CAT II) The DBA will ensure applications that access the database are not used with options that display the database account password on the command line.			

4.35 DG0069: Production data import to development DBMS

Description: Data export from production databases may include sensitive data. Application developers do not have a need to know to sensitive data. Any access they may have to production data would be considered unauthorized access and subject the sensitive data to unlawful or unauthorized disclosure.

Check:

If the database being reviewed is not a production database, this check is Not Applicable.

Review procedures or restrictions for data exports from the production database. If data exports are not allowed, then review methods for preventing and monitoring of any production data export.

If procedures and methods are not complete or implemented, this is a Finding.

Acknowledgement of data export restrictions and procedures by individuals granted privileges that enable data export is considered sufficient protection, however, record of such acknowledgement must be filed.

Privileges required for database copy and/or export commands include sysadmin, dbcreator or database owner of the source database.

If DBMS export utilities are not restricted to users authorized by the IAO, this is a Finding.

Fix:

Document procedures and restrictions for production data export.

Require any users assigned privileges that allow the export of production data from the database to acknowledge understanding of the export restrictions.

Restrict permissions allowing use or access to database export procedures or functions to authorized users.

VKEY: V0015140	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECAN	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0069: CAT II) The DBA will ensure production data is not exported for import to development databases except in accordance with processes and procedures approved by the Information Owner.			

4.36 DG0070: DBMS user account authorization

Description: Unauthorized user accounts provide unauthorized access to the database and may allow access to database objects. Only authorized users should be granted database accounts.

Check:

Review procedures for ensuring authorization of new or re-assigned DBMS user accounts. Requests for user account access to the DBMS should include documented approval by an authorized requestor. Procedures should also include notification for a change in status, particularly cause for revocation of account access, to any DBMS accounts.

Review the user accounts listed either in the script report or manually against the authorized user list.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT l.name
FROM [master].dbo.sysusers u, [master].dbo.syslogins l
WHERE u.uid = l.sid
AND (l.isntuser = 1 OR l.isntname = 0)
AND l.sid <> 0x01
ORDER BY l.name
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM sys.server_principals
WHERE type IN ('S', 'U')
AND principal_id <> 1
ORDER BY name
```

If procedures for DBMS user account authorization are incomplete or not implemented, this is a Finding.

If any accounts listed are not clearly authorized, this is a Finding.

Fix:

Develop, document and implement procedures for authorizing creation and changes to user accounts. Monitor user accounts to verify that they remain authorized. Drop user accounts that are no longer authorized.

VKEY: V0002508	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAAC	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.24			
STIG Requirement:	(DG0070: CAT II) The DBA will ensure unauthorized database accounts are removed or disabled.			

4.37 DG0071: DBMS password change variance

Description: Changing passwords frequently can thwart password-guessing attempts or re-establish protection of a compromised DBMS account. Minor changes to passwords may not accomplish this as password guessing may be able to continue to build on previous guesses or the new password may be easily guessed using the old password.

Check:

If no DBMS accounts authenticate using passwords, this check is Not a Finding.

If DBMS uses Windows Authentication only, this check is Not a Finding.

If the DBMS does not natively support this functionality, this check is Not a Finding.

Note: This functionality can be added to SQL Server programmatically, but is not addressed here.

If the DBMS supports this functionality, review the settings and function logic or have the DBA demonstrate a password change to ensure that the function requires new passwords to differ from old passwords by more than four characters.

If the review or the demonstration reveals that passwords are not checked for a difference of more than four characters, this is a Finding.

Fix:

Define, configure and test a password verify feature or function that authenticates passwords on change to ensure that new password differs from old password by more than four characters.

VKEY: V0003815	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2.2			
STIG Requirement:	(DG0071: CAT II) The DBA will ensure database passwords differ from previous values by more than 4 characters when changed where supported by the DBMS.			

4.38 DG0072: DBMS Password change time limit

Description: Frequent password changes may indicate suspicious activity or attempts to bypass password controls based on password histories. Limiting the frequency of password changes helps to enforce password change rules and can lead to the discovery of compromised accounts.

Check:

If no DBMS accounts authenticate using passwords, this check is Not a Finding.

If DBMS uses Windows Authentication only, this check is Not a Finding.

If the DBMS does not natively support this functionality, this check is Not a Finding.

Note: This functionality can be added to SQL Server programmatically, but is not addressed here.

If the DBMS supports this functionality, review the settings and function logic or have the DBA demonstrate a password change to ensure that the function does not allow user changes to passwords to occur more than once within a 24-hour period.

If the review or the demonstration reveals that passwords can be changed by users more than once within a 24-hour period, this is a Finding.

Fix:

Define, configure and test a password verify feature or function that authenticates passwords on change to ensure that changes to passwords do not occur more than once within a 24-hour period.

VKEY: V0015612	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2.2			
STIG Requirement:	(DG0072: CAT II) The DBA will ensure users are not allowed to change their database account passwords more than once every 24 hours without IAO approval where supported by the DBMS. (This requirement does not apply to password changes after password reset actions initiated by the DBA or application administrator).			

4.39 DG0074: DBMS inactive accounts

Description: Unused or expired DBMS accounts provide a means for undetected, unauthorized access to the database.

Check:

Review procedures and implementation for monitoring the DBMS accounts for expiration or inactivity.

Note: SQL Server does not maintain login statistics within the DBMS. This functionality can be added to SQL Server programmatically and is not addressed here.

For SQL Server 7 & 2000:

```
SELECT l.name
FROM [master].dbo.syslogins l, [master].dbo.sysusers u
WHERE l.sid = u.uid
AND u.issqluser = 1
ORDER BY l.name
```

Compare the accounts against audit records to determine account usage.

Verify that any accounts that have been inactive or expired for longer than 30 days are authorized to remain. If any are not, this is a Finding.

For SQL Server 2005:

Review login accounts defined for the instance:

```
SELECT name
FROM [master].sys.server_principals
WHERE type = 'S'
ORDER BY name
```

Compare the accounts against audit records to determine account usage.

Verify that any accounts that have been inactive or expired for longer than 30 days are authorized to remain. If any are not, this is a Finding.

Fix:

Develop and implement procedures to monitor database accounts for inactivity or expiration. Investigate and authorize if appropriate any accounts that are expired or have been inactive for more than 30 days.

Where appropriate, protect authorized expired or inactive accounts by disabling them or applying some other similar protection.

Note: DBMS accounts using Windows Authentication or linked to certificates can be monitored or managed by the host or through Active Directory for domain accounts. Ensure DBA and SA coordinate host/domain account management and host/domain account management meets host/domain-level STIG requirements.

VKEY: V0015130	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: IAAC	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.24			
STIG Requirement:	(DG0074: CAT II) The DBA will monitor database account expiration and inactivity and remove expired accounts and accounts that are inactive for 35 days or longer or the site maximum limit.			

4.40 DG0075: DBMS links to external databases

Description: DBMS links provide a communication and data transfer path definition between two databases that may be used by malicious users to discover and obtain unauthorized access to remote systems. Database links between production and development DBMSs provide a means for developers to access production data not authorized for their access or to introduce untested or unauthorized applications to the production database. Only protected, controlled, and authorized downloads of any production data to use for development should be allowed. Only applications that have completed the configuration management process should be introduced by the application object owner account to the production system.

Check:

If this is not a production database, this check is Not Applicable.

Note: SQL Server check DG0190 addresses authorization of all defined remote and linked databases.

Review documentation for definitions of authorized external interfaces. The documentation should include:

1. Any remote access to the database
2. The purpose or function of the remote connection,
3. Any access to data or procedures stored externally to the local DBMS
4. Any network ports or protocols used by remote connections
5. Whether the remote connection is to a production, test, or development system
6. Any security accounts used by DBMS to access remote resources or objects

To view remote and linked servers:

For SQL Server 7 & 2000:

```
SELECT srvname
FROM [master].dbo.sysservers
WHERE srvid <> 0
ORDER BY srvname
```

For SQL Server 2005:

```
SELECT name
FROM [master].sys.servers
WHERE server_id <> 0
ORDER BY name
```

If any database links are defined between the production database and any test or development databases, this is a Finding.

If the documentation for remote interfaces does not exist or is incomplete in the System Security Plan and AIS Functional Architecture documentation, this is a Finding.

Fix:

Document all remote or external interfaces used by the DBMS to connect to or allow connections from remote or external sources in the System Security Plan and AIS Functional Architecture documentation. Include with the documentation as appropriate, any network ports or protocols, security accounts, and the sensitivity of any data exchanged.

Do not define or configure database links between production databases and test or development databases.

Delete any links or remote server definitions between production and test or development databases.

VKEY: V0003818	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DFCA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0075: CAT II) The DBA will ensure database connections to remote databases or remote or external applications and services are disabled and/or not defined unless database replication is in use or the remote connection is mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.41 DG0076: Sensitive data import to development DBMS

Description: Data export from production databases may include sensitive data. Application developers do not have a need to know to sensitive data. Any access they may have to production data would be considered unauthorized access and subject the sensitive data to unlawful or unauthorized disclosure. See DODD 8500.1 section E2.1.41 for a definition of Sensitive Information.

Check:

If the database is not a production database, this check is Not Applicable.

Review procedures or restrictions for data exports from the production database. If data exports are allowed, then review procedures for protecting any sensitive data included in the exports. If sensitive data is included in the exports and no protections are taken to remove or modify the data to render it not sensitive when provided to unauthorized users, this is a Finding.

Fix:

Document procedures and restrictions for production data export. Require any users assigned privileges that allow the export of production data from the database to acknowledge understanding of the export restrictions. Restrict permissions allowing use or access to database export procedures or functions to authorized users.

VKEY: V0003819	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECAN	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0076: CAT II) The DBA will ensure sensitive application data exported from the database for import to remote databases or applications is not provided to personnel or applications not authorized or approved by the Information Owner.			

4.42 DG0077: Production data protection on a shared system

Description: Developers granted elevated database, operating system privileges on systems that support both development, and production databases can affect the operation and/or security of the production database system. Operating system and database privileges assigned to developers on shared development and production systems should be restricted.

Check:

Review the list of instances and databases installed on the host system with the DBA. Ask which databases are production databases and which are for development.

If only development or only production databases exist on this host, this is Not a Finding.

Otherwise, ask the DBA to confirm that policy and procedures are in place for the IAO to review database and operating system privileges on the system. If none is in place, this is a Finding.

Ask the DBA/SA if developer host accounts have been granted privileges to production database directories, files or resources. If they have been, this is a Finding.

Fix:

Develop, document and implement procedures to review and maintain privileges granted to developers on shared production and development host systems and databases.

VKEY: V0003820	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0077: CAT II) The DBA will ensure developers are not granted system privileges within a production database.			

4.43 DG0078: DBMS individual accounts

Description: Use of accounts shared by multiple users, applications, or processes limit the accountability for actions taken in or on the data or database. Individual accounts provide an opportunity to limit database authorizations to those required for the job function assigned to each individual account.

Check:

Review DBMS account names against the list of authorized DBMS accounts in the System Security Plan. If any accounts indicate use by mulitiple persons that are not mapped to a specific person, this is a Finding.

If any applications or processes share an account that could be assigned an individual account or are not specified as requiring a shared account, this is a Finding.

Note: Privileged installation accounts may be required to be accessed by DBA or other administrators for system maintenance. In these cases, each use of the account must be logged in some manner to assign accountability for any actions taken during the use of the account.

Fix:

Create individual accounts for each user, application, or other process that requires a database connection.

Document any accounts that are shared where separation is not supported by the application or for maintenance support.

Design, develop and implement a method to log use of any account to which more than one person has access. Restrict interactive access to shared accounts to the fewest persons possible.

VKEY: V0015613	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: IAIA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2			
STIG Requirement:	(DG0078: CAT II) The DBA will ensure database user accounts are configured to require individual authentication in order to connect to the DBMS.			

4.44 DG0079: DBMS password complexity

Description: Weak passwords are a primary target for attack to gain unauthorized access to databases and other systems. Where username/password is used for identification and authentication to the database, requiring the use of strong passwords can help prevent simple and more sophisticated methods for guessing at passwords.

Check:

If SQL server is configured for Windows Authentication only, this check is Not a Finding.

If the server is configured to allow SQL Server Authentication, verify passwords are checked for complexity requirements where DBMS version permits:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT s.name
FROM [master].dbo.syslogins s, [master].dbo.sysusers u
WHERE s.sid = u.sid
AND s.sid <> 0x01
AND u.issqluser = 1
ORDER BY s.name
```

Perform manual verification of password complexity requirements. If any accounts do not comply with established password policies, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.sql_logins
WHERE type = 'S'
AND is_policy_checked <> '1'
ORDER BY name
```

If any rows are returned, this is a Finding.

Fix:

For SQL Server 7 & 2000:

For all DBMS accounts using SQL Server logins, develop, document, implement policy and procedures and periodically ensure SQL Server account passwords meet DoD password complexity requirements.

For SQL Server 2005:

For all DBMS accounts using SQL Server logins, set the accounts for password complexity checking:

From the query prompt:

```
ALTER LOGIN [login name] CHECK_POLICY = ON
```

Note: This setting depends upon host system password complexity settings. The host system must be configured to comply with Windows STIG requirements.

VKEY: V0015152	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: IAIA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2.2			
STIG Requirement:	(DG0079: CAT II) The DBA will ensure database password complexity standards meet current minimum requirements for length (9 characters or more for database application user accounts and 15 characters or more for privileged database accounts) and composition (at least two uppercase characters, two lowercase characters, two special characters, two digits) where supported by the DBMS.			

4.45 DG0080: DBMS application user privilege assignment review

Description: Users granted privileges not required to perform their assigned functions are able to make unauthorized modifications to the production data or database. Monthly or more frequent periodic review of privilege assignments assures that organizational and/or functional changes are reflected appropriately.

Check:

Review procedures and implementation evidence to determine if procedures are in place for periodic review of user privileges by the IAO. Evidence may consist of email or other correspondence that acknowledges receipt of periodic reports and notification of review between the DBA and IAO or other auditors as assigned.

If the procedures are incomplete or no evidence of implementation exists, this is a Finding.

Fix:

Develop, document and implement procedures for periodic review of application user database privilege assignments. Include methods to provide evidence of review in the procedures to verify reviews occur in accordance with the procedures.

VKEY: V0003821	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0080: CAT II) The DBA will ensure privileges granted to application user database accounts are restricted to those required to perform the specific application functions.			

4.46 DG0083: DBMS audit report automation

Description: Audit record collection may quickly overwhelm storage resources and an auditor's ability to review it in a productive manner. Automated tools can provide the means to manage the audit data collected as well as present it to an auditor in an efficient way.

Check:

Review automated tool usage for reporting of audit trail data.

If automated tools are not used, this is a Finding.

Automated DBMS jobs and/or procedures may be used to produce the periodic reports.

Fix:

Develop, document and implement database or host system procedures to report audit trail data in a form usable to detect unauthorized access to or usage of DBMS privileges, procedures or data.

VKEY: V0015102	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECRG	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.17			
STIG Requirement:	(DG0083: CAT II) The IAO will ensure automated tools are available and implemented for review and reporting of DBMS audit records.			

4.47 DG0084: DBMS residual data clearance

Description: Database storage locations may be reassigned to different objects during normal operations. If not cleared of residual data, sensitive data may be exposed to unauthorized access. SQL Server common criteria compliance enables the following functions in SQL Server: 1) enables overwrite of memory storage before reuse, 2) enables login statistic auditing including the maintenance of last successful and unsuccessful login, 3) enables the precedence of the DENY column privilege assignment over the GRANT column privilege assignment where both may be assigned simultaneously. These features protect against respectively: 1) potential disclosure of sensitive information that may reside in reallocated memory space, 2) undiscovered unauthorized login attempts and 3) inadvertent assignment of unauthorized privileges.

Check:

For SQL Server 2005:

Determine the SQL Server Edition:

From the query prompt:

```
SELECT CONVERT(INT, SERVERPROPERTY('EngineEdition'))
```

If value returned is 1 (Personal or Desktop Edition), 2 (Standard Edition) or 4 (Express Edition), this check is Not Applicable.

From the query prompt:

```
SELECT CAST(value AS INT)
FROM [master].sys.configurations
WHERE name = 'common criteria compliance enabled'
```

If the value = 0, confirm in the System Security Plan that common criteria compliance is documented as not required by the IAO. If it is not documented or is required and approved, this is a Finding.

Fix:

For SQL Server 2005:

Authorize and document requirements for use of the common criteria compliance option in the System Security Plan and AIS Functional Architecture documentation. Where authorized, enable its use.

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'common criteria compliance enabled', 1
```

RECONFIGURE

VKEY: V0015614	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECRC	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.16			
STIG Requirement:	(DG0084: CAT III) The DBA will ensure DBMS resource controls are enabled to clear residual data from released object stores.			

4.48 DG0085: Minimum DBA privilege assignment

Description: The default DBA privileges typically include all privileges defined for a DBMS. These privileges are required to configure the DBMS and to provide other users access to DBMS objects. However, DBAs may not require access to application data or other privileges to administer the DBMS. Where not required or desired, DBAs may be prevented from accessing protected data for which they have no need-to-know or from utilizing unauthorized privileges for other actions. Although DBAs may assign themselves privileges to override any restrictions, the assignment of privileges is an audit requirement and this auditable event may assist discovery of a misuse of privileges.

Check:

Review privileges assigned to the DBA roles and compare them to those listed in the System Security Plan with the IAO.

If privileges are granted to DBAs that are not listed as required privileges in the System Security Plan, this is a Finding.

Note: If the number of DBAs appears excessive to for the same job function, then query the DBA to discover if separating DBA roles by specific job function is in order. Query the DBA or IAO to determine the advisability of having only one DBA job function defined.

If security would be enhanced by separating DBA responsibilities into separate job functions with custom DBA roles, this is Not a Finding.

Fix:

Limit privileges assigned to DBA roles.

Document DBA job functions and minimum privileges required to perform the DBA job function in the System Security Plan.

Where many DBAs administer the same DBMS, consider dividing DBA job functions to restrict DBAs to administering a smaller portion of the DBMS to prevent intentional or inadvertent modification to the entire DBMS or specific portions.

VKEY: V0015615	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: IAO/DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0085: CAT II) The DBA will ensure the minimum database administrative privileges are assigned to database administrative roles to perform the administrative job function.			

4.49 DG0086: DBMS DBA role privilege monitoring

Description: Excess privilege assignment can lead to intentional or unintentional unauthorized actions. Such actions may compromise the operation or integrity of the DBMS and its data.

Check:

Review procedures and implementation evidence of DBA role privilege monitoring.

If procedures are incomplete or not implemented, this is a Finding.

If monitoring does not occur every 30 days or more often, this is a Finding.

Fix:

Design and implement procedures for monitoring DBA role privilege assignments.

VKEY: V0015106	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0086: CAT II) The IAO will review monthly or more frequently the database privileges assigned to database administrative roles to ensure they are limited to the minimum required.			

4.50 DG0087: DBMS sensitive data labeling

Description: The sensitivity marking or labeling of data items promotes the correct handling and protection of the data. Without such notification, the user may unwittingly disclose sensitive data to unauthorized users.

Check:

If the DBMS does not provide the capability to mark or label sensitive data within the DBMS, this check is Not a Finding.

For SQL Server 2005:

Review the DBMS configuration for marking and labeling of sensitive data. If sensitive data is not marked and labeled in accordance with the System Security Plan, this is a Finding.

http://www.microsoft.com/technet/prodtechnol/sql/2005/multisec.mspx

Fix:

For SQL Server 2005:

Employ DBMS capabilities to mark or label sensitive data stored within the DBMS where supported. Document the appropriate markings of sensitive data in the System Security Plan.

VKEY: V0015616	Severity: CAT 3		Policy: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECML	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.12			
STIG Requirement:	(DG0087: CAT III) The DBA will configure DBMS marking and labeling of non-public data where required in accordance with the System Security Plan.			

4.51 DG0088: DBMS vulnerability mgmt and IA compliance testing

Description: The DBMS security configuration may be altered either intentionally or unintentionally over time. The DBMS may also be the subject of published vulnerabilities that require the installation of a security patch or a reconfiguration to mitigate the vulnerability. If the DBMS is not monitored for required or unintentional changes that render it not compliant with requirements, then it can be vulnerable to attack or compromise.

Check:

Review procedures and evidence of implementation for DBMS IA and vulnerability management compliance.

If the DBMS is not monitored for compliance, this is a Finding.

Fix:

Develop, document and implement procedures for periodic testing of the DBMS for current vulnerability management and security configuration compliance.

VKEY: V0015112	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECMT	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.13			
STIG Requirement:	(DG0088: CAT III) The IAO will ensure the DBMS is included in the periodic testing of conformance with vulnerability management and IA configuration requirements.			

4.52 DG0089: Developer DBMS privileges on production databases

Description: Developers play a unique role and represent a specific type of threat to the security of the DBMS. Where restricted resources prevent the required separation of production and development DBMS installations, developers granted elevated privileges to create and manage new database objects must also be prevented from actions that can threaten the production operation.

Check:

If the database is not a production database, this check is Not Applicable.

Review privileges assigned to developers:

1. Identify login name of developer DBMS accounts from the System Security Plan and/or DBA.
2. For each developer account, display the username SID and the databases where the user is defined:

   EXEC SP_HELPLOGINS '[login name]'

3. Display all fixed server role membership assignments:

   EXEC SP_HELPSRVROLEMEMBER

If developers are assigned privileges that allow change or alteration of database objects in any production databases, this is a Finding.

If developers are assigned membership to any DBMS server roles, this is a Finding.

Fix:

Revoke DBA privileges assigned to developers on production DBMS unless required and authorized.

Revoke database or other production object administrative privileges from developers unless required and authorized.

Restrict developer privileges to production objects to those granted to application users only where such privileges are required and authorized.

VKEY: V0015114	Severity: CAT 3		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECPC	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.15			
STIG Requirement:	(DG0089: CAT III) The DBA will ensure application developer database accounts are assigned limited privileges in order to protect production application objects.			

4.53 DG0090: DBMS sensitive data identification and encryption

Description: Sensitive data stored in unencrypted format within the database is vulnerable to unauthorized viewing.

Check:

If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan and/or AIS Functional Architecture documentation, this check is Not a Finding.

Have your DBA use select statements in the database to review sensitive data stored in tables as identified in the System Security Plan and/or AIS Functional Architecture documentation.

If any sensitive data is human readable by unauthorized users, this is a Finding.

Note: The result for this check may be marked as Not a Finding and the requirement of encryption in the database waived where the database has only database administrative accounts and application accounts that have a need-to-know to the data. This waiver does not preclude any requirement for encryption of the associated database data file (see DG0092).

Fix:

Use third-party tools or native DBMS features to encrypt sensitive or classified data stored in the database. Use only FIPS 140-2 validated encryption libraries or modules to provide encryption.

Document acceptance of risk by the Information Owner where sensitive or classified data is not encrypted. Have the IAO document assurance that the unencrypted sensitive or classified information is otherwise inaccessible to those who do not have Need-to-Know access to the data.

Developers should consider using a record-specific encryption method to protect individual records. For example, by employing the session username or other individualized element as part of the encryption key, then decryption of a data element is only possible by that user or other data accessible only by that user.

Consider applying additional auditing of access to any unencrypted sensitive or classified data when accessed by users (with and/or without Need-to-Know).

VKEY: V0015131	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECCR	Check Type: Manual	Database Level: False	Responsibility: IAO/DBA	Documentable: False
Reference:	Database STIG 3.3.5			
STIG Requirement:	(DG0090: CAT II) The IAO/DBA will ensure sensitive data is encrypted within the database where required by the Information Owner.			

4.54 DG0092: DBMS data file encryption

Description: Where access controls do not provide complete protection of sensitive or classified data, encryption can help to close the gap. Encryption of sensitive data helps protect disclosure to privileged users who do not have a need-to-know requirement to view the data that is stored in files outside of the database. Data encryption also provides a level of protection where database controls cannot restrict access to single rows and columns of data.

Check:

Review the System Security Plan and/or the AIS Functional Architecture documentation to discover sensitive or classified data identified by the Information Owner that requires encryption.

If no sensitive or classified data is identified as requiring encryption by the Information Owner, this check is Not a Finding.

Have the DBA use select statements in the database to review sensitive data stored in tables as identified in the System Security Plan and/or AIS Functional Architecture documentation.

If all sensitive data as identified is encrypted within the database objects, this is Not a Finding.

If sensitive data is not encrypted within the database objects, then review encryption applied to the DBMS host data file. If no encryption is applied, this is a Finding.

Consider which data files store the sensitive data files. Not all DBMS data files will require encryption.

In addition, review the check for DG0090.

Fix:

Use third party or native OS/DBMS encryption to encrypt DBMS data files that store sensitive or classified data as required by the Information Owner. To lessen the impact on system performance, separate sensitive data where file encryption is required into dedicated data files.

VKEY: V0015132	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECCR	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.5			
STIG Requirement:	(DG0092: CAT II) The DBA will ensure database data files are encrypted where encryption of sensitive data within the DBMS is not available.			

4.55 DG0093: Remote administrative connection encryption

Description: Communications between a client and database service across the network may contain sensitive information including passwords. This is particularly true in the case of administrative activities. Encryption of remote administrative connections to the database ensures confidentiality of configuration, management, and other administrative data.

Check:

If no administration accounts are accessed remotely, this check is Not a Finding.

Ask the DBA if access to the administration accounts is:

1. Made using remote access through a local host account
2. Made directly to the database from a remote database client

If access is via a local host account, review procedures, policy, and/or evidence that remote administrative account access is performed only via an encrypted connection protocol such as SSH, Remote Desktop Connection (properly configured, of course), etc., to connect to the host. If it is not, this is a Finding.

If access is via direct connection to the DBMS from a DBMS client, confirm that a dedicated database listener exists on the DBMS server and configured to encrypt communications for remote administrative connections. If it is not, this is a Finding.

If there are any listeners on the DBMS host that are configured to accept unencrypted traffic, determine through review of policy and training evidence that DBAs know to use and do use the encrypted listener for remote access to administrative accounts. If no such policy exists, the DBAs have not been instructed to use or do not use an encrypted connection, this is a Finding.

Interview DBAs to confirm they use the encrypted listener for remote DBA access. If any DBAs do not, this is a Finding.

Fix:

Do not administer DBMS systems remotely if possible. If this is not possible, ensure that all connections to the DBMS for administrative purposes utilize encryption at all possible levels [i.e. Network (VPN), Host (SSH/RDP), and Database (Client/ODBC/listener)].

VKEY: V0003825	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECCT / ECNK	Check Type: Interview	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.6			
STIG Requirement:	(DG0093: CAT II) The DBA will ensure remote administrative connections to the database are encrypted.			

4.56 DG0095: DBMS audit trail data review

Description: Review of audit trail data provides a means for detection of unauthorized access or attempted access. Frequent and regularly scheduled reviews ensure that such access is discovered in a timely manner.

Check:

Review policy, procedures and implementation evidence for daily audit trail monitoring.

For SQL Server, the audit trail data is found in audit traces, the system error logs (ERRORLOG.*) files, and the system and application event logs.

If the policy, procedures and evidence are not present or complete, this is a Finding.

Fix:

Develop, document and implement policy and procedures to monitor audit trail data daily.

VKEY: V0003827	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAT	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.3			
STIG Requirement:	(DG0095: CAT II) The IAO will ensure the database audit data is reviewed daily to discover suspicious or unusual activity.			

4.57 DG0096: DBMS IA policy and procedure review

Description: A regular review of current database security policies and procedures is necessary to maintain the desired security posture of the DBMS. Policies and procedures should be measured against current DOD policy, STIG guidance, vendor-specific guidance and recommendations, and site-specific or other security policy.

Check:

Review policy, procedures and implementation evidence of annual reviews of DBMS IA policy and procedures.

If policy and procedures do not exist, are incomplete, or are not implemented and followed annually or more frequently, this is a Finding.

Fix:

Develop, document and implement policy and procedures to review DBMS IA policies and procedures on an annual or more frequent basis.

VKEY: V0015138	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCAR	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.1			
STIG Requirement:	(DG0096: CAT III) The IAO will ensure database IA policies and procedures are reviewed at least annually and are current and consistent with all IA requirements.			

4.58 DG0097: DBMS testing plans and procedures

Description: Updates and patches to existing software have the intention of improving the security or enhancing or adding features to the product. However, it is unfortunately common that updates or patches can render production systems inoperable or even introduce serious vulnerabilities. Some updates also set security configurations back to unacceptable settings that do not meet security requirements. For these reasons, it is a good practice to test updates and patches offline before introducing them in a production environment.

Check:

Review policy, procedures and implementation evidence for testing DBMS installations, upgrades and patches prior to production deployment.

If policy and procedures do not exist, are incomplete or evidence of implementation does not exist, this is a Finding.

Fix:

Develop, document and implement policy and procedures for testing DBMS installations, upgrades and patches prior to deployment on production systems.

VKEY: V0015139	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCCT	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.3			
STIG Requirement:	(DG0097: CAT II) The IAO will ensure comprehensive testing plans and procedures for database installations, updates, and patches are defined and implemented before being deployed in a production environment.			

4.59 DG0098: DBMS access to external local objects

Description: Objects defined within the database, but stored externally to the database are accessible based on authorizations defined by the local operating system or other remote system that may be under separate security authority. Access to external objects may thus be uncontrolled or not based on least privileges defined for each user job function. This in turn may provide unauthorized access to the external objects.

Check:

Review the database for definitions of application objects stored externally to the database.

Determine if there are methods to disable use or access or to remove definitions for external data objects.

If there are ways to prevent access to the external application data objects or the requirement for their access is not documented in the AIS functional architecture, this is a Finding.

Fix:

Include any external application data objects defined in the database that is required for authorized application use in the AIS functional architecture documentation.

Disable use of or remove any external application data object definitions that are not authorized.

VKEY: V0015617	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0098: CAT II) The DBA will configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.60 DG0099: DBMS access to external local executables

Description: DBMSs may spawn additional external processes to execute procedures that are defined in the DBMS, but stored in external host files (external procedures). The spawned process used to execute the external procedure may operate within a different OS security context than the DBMS and provide unauthorized access to the host system.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysobjects
WHERE xtype = 'X'
ORDER BY name
```

Verify with the DBA that all procedures listed are system-defined. Review extended stored procedure create dates and names to determine consistency with other extended stored procedures.

Verify that any extended stored procedures listed have their use documented in the System Security Plan as required for operation and authorized by the IAO. If any are not, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.system_objects
WHERE type = 'X'
ORDER BY name
```

Review the list of extended stored procedures returned.

Verify that any extended stored procedures listed have their use documented in the System Security Plan as required for operation and authorized by the IAO. If any are not, this is a Finding.

Fix:

Restrict access of extended stored procedures to SYSADMINs where required.

Note: Use of some extended stored procedures is required for common use and removal may affect SQL Server operations. The requirement differs based on SQL Server usage. To determine required extended stored procedures for a

specific SQL Server installation, enable auditing on execute of the procedures. Review the audit data after a sufficient period to capture all operational usage, and then restrict access to unused extended stored procedures. If no operational issues arise after a sufficient time (you should double the period used before), remove the unused extended stored procedures.

By default, the public role is granted execute access to many system-supplied extended stored procedures. It is recommended these execute privileges to extended stored procedures (the ones being retained for system use) be transferred from the public role and re-assigned to a custom all-user group.

To view a list of extended stored procedures to which public has been granted execute access:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT OBJECT_NAME(p.id)
FROM [master].dbo.sysprotects p, [master].dbo.sysobjects o
WHERE p.id = o.id
AND USER_NAME(p.uid) = 'public'
AND action = 224
AND protecttype IN (204, 205)
ORDER BY OBJECT_NAME(p.id)
```

For SQL Server 2005:

From the query prompt:

```
SELECT o.name
FROM [master].sys.system_objects o, [master].sys.database_permissions p
WHERE o.object_id = p.major_id
AND o.type = 'X'
AND p.state IN ('G', 'W')
AND p.grantee_principal_id = 0
ORDER BY o.name
```

Redesign applications stored in extended stored procedures to use CLR integration [for SQL Server 2005 and later].

VKEY: V0015618	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.61 DG0100: DBMS replication account privileges

Description: Replication accounts may be used to access databases defined for the replication architecture. An exploit of a replication on one database could lead to the compromise of any database participating in the replication that uses the same account name and credentials. If the replication account is compromised and it has DBA privileges, the database is at additional risk to unauthorized or malicious action.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
USE master
EXEC SP_GET_DISTRIBUTOR
```

If the value of installed is 0, and a review of the System Security Plan confirms the use of replication is not required and not allowed, this check is Not Applicable.

If the value of installed is 1, and a review of the System Security Plan confirms the use of replication is required and allowed, this is Not a Finding. If it is not required or not allowed, this is a Finding.

OR

From the SQL Server Enterprise Manager GUI:

1. Right-click on SQL Server
2. Select Properties
3. Select Replication tab

If the notice, "ServerName is not configured as a Publisher or Distributor" is displayed, and Replication is listed in the System Security Plan and AIS Functional Architecture as not required or allowed, this check is Not Applicable.

If SQL Server is configured as a Distributor and/or publisher, from the Replication tab:

4. Click on the Configure button
5. Select the Publishers tab
6. Click on the button in the publisher record
7. Make a note of the snapshot folder path

Review Distributor Security.

From the SQL Server Enterprise Manager GUI:

1. Select Tools from menu bar
2. Select Replication
3. Select Configure Publishing, Subscribers, and Distribution
4. Select subscribers tab
5. Double-click on each subscriber
6. Select Agent connection to the subscriber
7. View Impersonate the SQL Server Agent account on SQL Server (trusted connection)
8. Repeat for each subscriber listed
9. Repeat for each Publisher listed under Publisher tab

If any subscriber or publishers do not have Impersonate selected, this is a Finding.

Review Snapshot Folder Security.

From the SQL Server Enterprise Manager GUI:

1. Connect/expand SQL Server
2. Expand Replication
3. Expand Publications
4. For each publication:
5. Right-click on publication
6. Select Properties
7. Select Snapshot location tab
8. Note snapshot location specification

If no snapshot folders are listed for any databases, this is Not a Finding.

If the default snapshot folder location is selected, the publication is using the snapshot folder noted above.

The following check must be verified from the OS SRR information or done from the host system console.

For each Snapshot folder noted above:

From Windows Explorer:

1. Browse to snapshot folder noted from above
2. Right-click on directory
3. Select Properties
4. Select Security tab
5. Select Permissions

If snapshot folder is a Network Share directory, this is a Finding.

If snapshot folder permissions are other than Full Control to Administrators, the custom DBA group, CREATOR OWNER, SYSTEM and read/write to SQL Server service accounts, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
USE master
EXEC SP_GET_DISTRIBUTOR
```

If the value of installed is 0, and a review of the System Security Plan confirms the use of replication is not required and not allowed, this check is Not Applicable.

If the value of installed is 1, and a review of the System Security Plan confirms the use of replication is required and allowed, this is Not a Finding. If it is not required or not allowed, this is a Finding.

The following steps determine if the security of the configured Replication follows best practices:

From the query prompt:

```
EXEC SP_HELPREPLICATIONDBOPTION
```

1. Ensure replication data is encrypted in transit

   Review documentation and evidence of configuration for encrypted connections between remote databases participating in replication where transmissions cross untrusted (support connections that do not have a need-to-know access requirement to the data being replicated) networks.

2. Confirm replication agents use dedicated accounts

   This is covered individually under check DM6065 and is not included in Finding status here. To view replication agent accounts:

   ```
   USE msdb
   SELECT p.name 'Proxy Name', c.credential_identity
   FROM sys.credentials c, sysproxies p, sysproxysubsystem s
   WHERE c.credential_id = p.proxy_id
   AND s.proxy_id = p.proxy_id
   ```

AND s.subsysstem_id > 3
AND s.subsystem_id < 9

3. Confirm Replication Agent accounts are assigned minimum privileges

   For each database, review assigned roles/permissions for each agent account:

   USE [database name]

   For each agent account listed under #2 above:

   EXEC SP_HELPUSER '[user name]'

   If any GroupName other than db_owner is listed in any database, this is a Finding.

   If any GroupName is listed in any database other than replication databases, this is a Finding

   EXEC SP_HELPROTECT '[user name]'

   If any permission is listed, this is a Finding.

   Perform once:

   EXEC SP_HELPSRVROLEMEMBER

   If any replication agent accounts are listed, this is a Finding.

4. Confirm only authorized Merge and Distribution Agent accounts are listed in the Publication Access List (PAL)

   For each replication database:

   EXEC SP_HELPPUBLICATION

   For each publication listed:

   EXEC SP_HELP_PUBLICATION_ACCESS '[publication name]'

   If any accounts are listed under publications that are not SYSADMINs, replication merge (category REPL-Merge) or replication distributor (category REPL-Distribution) agent accounts, this is a Finding.

5. Confirm minimum permissions are assigned to any local snapshot folders

Results for this security check are recorded individually under DM6075.

6. (cont from 5) Confirm snapshot Agent accounts are granted only write permissions to the snapshot folder

   If the snapshot agent account has more than write access to the snapshot folder, this is a Finding.

7. Verify network shares are used for snapshot folders accessed by pull subscriptions

   If the server does not have a Publisher database, this check is Not a Finding.

   For each publisher database:

   ```
   USE [database name]
   EXEC SP_HELPSUBSCRIPTION
   ```

   If any subscribers listed indicate a remote database (a database on a different server), then confirm the snapshot folder is defined as a network share. If it is not, this is a Finding.

   Note: See folder information for the publication listed for the subscriber under the SP_HELPPUBLICATION results. Windows shares are indicated with a share icon and are indicated as shared in the directory properties \ share tab.

8. Verify Agent accounts use Windows authentication

   See Agent accounts returned from #2 above

   If any accounts listed are not Windows accounts (display [domain or computername]\[account name]), this is a Finding.

Fix:

Disable replication if replication is not required.

For SQL Server 7 & 2000:

From the SQL Server Enterprise Manager GUI:

1. Right-click on SQL Server
2. Select Properties
3. Select Replication tab

4. Right-click on Replication
5. Click Disable Publishing and Distribution
6. Complete the steps presented

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Expand SQL Server
2. Right-click on Replication
3. Click Disable Publishing and Distribution
4. Complete the steps presented

Secure replication if required, authorized and documented.

For SQL Server 7 & 2000:

From the query prompt:

```
EXEC SP_BROWSESNAPSHOTFOLDER
```

From the SQL Server Enterprise Manager GUI:

1. Expand SQL Server
2. Expand Replication
3. Expand Publications
4. For each publication:
    a. Right-click on publication
    b. Select Snapshot location tab
    c. Select generate snapshots in the following location
    d. Enter the path to a secure folder that is not an Administrative share (same security as other SQL Server directories)
    e. De-select generate snapshots in the normal snapshot folder
    f. Click Apply
    g. Click OK

Verify Distributor Database security.

From the SQL Server Enterprise Manager GUI:

1. Select Tools from menu bar
2. Select Replication
3. Select Configure Publishing, Subscribers, and Distribution
4. Select subscribers tab
5. Double-click on each subscriber
6. Under Agent connection to the subscriber:

a. Select Impersonate the SQL Server Agent account on SQL Server (trusted connection)
b. Click OK
c. Repeat for each subscriber listed
d. Repeat for each Publisher listed under Publisher tab

For SQL Server 2005:

1. Create and use dedicated Windows-authenticated database accounts for Replication Agent use
2. Assign minimum database and file permissions to the Replication Agent accounts
3. Add only authorized Replication Merge and Distribution Agent accounts (and SYSADMIN accounts) to the PAL
4. Use network shared for snapshot folders access by pull subscriptions

Document replication in the System Security Plan, AIS Functional Architecture documentation and authorize with the IAO regardless of requirement.

VKEY: V0015169	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAN	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0100: CAT II) The DBA will ensure database accounts used for replication or distributed transactions are not granted DBA privileges.			

4.62 DG0101: DBMS external procedure OS account privileges

Description: External applications spawned by the DBMS process may be executed under OS accounts assigned unnecessary privileges that can lead to unauthorized access to OS resources. Unauthorized access to OS resources can lead to the compromise of the OS, the DBMS and any other service provided by the host platform.

Check:

View the Security Settings of the SQL Server service account to see user rights assigned to the service account or group.

To view assigned user rights (may be assigned using group privileges):

1. Click Start
2. Select Control Panel \ Administrative Tools (Win2K) or Select Administrative Tools (Win2K3)
3. Click Local Security Policy
4. Expand Local Policies
5. Select User Rights Assignment

For SQL Server Service account:

If any user rights are assigned to the service account other than the following, this is a Finding:

1. Log on as a service (SeServiceLogonRight)
2. Act as part of the operating system (SeTcbPrivilege) (Win2K only)
3. Log on as a batch job (SeBatchLogonRight)
4. Replace a process-level token (SeAssignPrimaryTokenPrivilege)
5. Bypass traverse checking (SeChangeNotifyPrivilege)
6. Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)

The following user rights are applicable for SQL Server 2005 only:

1. Permission to start SQL Server Active Directory Helper
2. Permission to Start SQL Write

Fix:

Create a local custom account for the SQL Server service accounts. A domain account may be used where network resources are required. Please see SQL Server Books Online for detailed information.

Assign the account to the SQL Server group (created at installation for SQL Server 2005) if available.

Assign the SQL Server account or group the user privileges as listed in the Check procedures.

VKEY: V0015620	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: SA / DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0101: CAT II) The DBA will ensure OS accounts used for execution of external database procedures have the minimum OS privileges required assigned to them.			

4.63 DG0102: DBMS services dedicated custom account

Description: Shared accounts do not provide separation of duties nor allow for assignment of least privileges for use by database processes and services. Without separation and least privilege, the exploit of one service or process is more likely to be able to compromise another or all other services.

Check:

Note: The SQL Server Service is covered in Check DG0101.

View the service account properties for the SQL Server services.

For SQL Server 7 & 2000:

1. Select Start / Administrative Tools / Services
2. View Properties / Log On for the following service:
    a. SQL Server Agent ([Instance Name])

If the SQL Server Agent service does not exist, this part of the check is Not a Finding.

If the SQL Server Agent service exists and does not use a custom account, this is a Finding.

If any of the services uses a domain user account, then review the requirement for the domain user account. If the service does not require interaction with network or domain resources, this is a Finding.

Note: Use of a local user account is recommended unless domain or network resources are accessed by the service.

For SQL Server 2005:

1. Select Start / Administrative Tools / Services
2. View Properties / Log On for the following services:
    a. SQL Server Agent ([Instance Name])
    b. SQL Server Analysis Services ([Instance Name])
    c. SQL Server Browser ([Instance Name])
    d. SQL Server FullText Search ([Instance Name])
    e. SQL Server Reporting Services ([Instance Name])
3. View Properties / Log on for the following services:
    a. SQL Server Active Directory Helper (Log On As Network Service)
    b. SQL Server Integration Services (Log On As Network Service)
    c. SQL Server VSS Writer (Log On As Local System)

Not all of these services may exist. If some services do not exist, checks for these services are Not a Finding.

If not all of the services use a custom account (with exception to 3a – 3c above), this is a Finding.

If any of the services uses a domain user account, then review the requirement for the domain user account. If the service does not require interaction with network or domain resources, this is a Finding.

Note: Use of a local user account is recommended unless domain or network resources are accessed by the service.

For SQL Server (all versions where applicable):

Review user rights assigned to the SQL Server service accounts. User rights may also be assigned to the service accounts via Windows groups and group policies:

1. Select Start / Run
2. Type: gpedit.msc (enter)
3. Under Group Policy Editor:
    a. Expand Local Computer Policy
    b. Expand Computer Configuration
    c. Expand Windows Settings
    d. Expand Security Settings
    e. Expand Local Properties
    f. Select User Rights Assignment
    g. Locate the Policies under each listed service
    h. Confirm the Security Setting for each policy contains the custom account assigned to the service
        i. Log on as a service
            1. SQL Server Agent
            2. SQL Server Analysis Services
            3. SQL Server Browser
            4. SQL Server FullText Search
            5. SQL Server Reporting Services
            6. SQL Server Active Directory Helper
            7. SQL Server Integration Services
            8. SQL Server VSS Writer
        ii. Act as part of the Operating System
            1. SQL Server Agent
        iii. Log on as a batch job
            1. SQL Server Agent
        iv. Bypass traverse checking
            1. SQL Server Agent
            2. SQL Server Integration Services

v. Replace a process-level token
    1. SQL Server Agent
vi. Adjust memory quotas for a process
    1. SQL Server Agent
vii. Create global objects
    1. SQL Server Integration Services
viii. Impersonate a client after authentication
    1. SQL Server Integration Services

i. Exit Group Policy Editor

If any user rights other than those listed above are assigned to the service accounts, this is a Finding.

Fix:

Create and assign custom local or domain user accounts to the SQL Server service accounts.

Disable any services and service accounts not required for operation.

Assign only required user rights to the custom service accounts.

Document in the System Security Plan

VKEY: V0015141	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DFCA	Check Type: Manual	Database Level: False	Responsibility: SA / DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0102: CAT II) The DBA will ensure each database service or process runs under a custom, dedicated OS account that is assigned the minimum privileges required for operation where applicable.			

4.64 DG0104: DBMS service identification

Description: Local or network services that do not employ unique or clearly identifiable targets can lead to inadvertent or unauthorized connections.

Check:

Review the SQL Server database names on the DBMS host:

Go to Start / Administrative Tools / Services

View service names that begin with "SQL Server". The database name is in parenthesis (NAME).

If database names as listed do not clearly identify the use of the database or clearly differentiate individual databases, this is a Finding.

An example of database naming that meets the requirement:

prdinv01 (Production Inventory Database #1)
dvsales02 (Development Sales Database #2)
msfindb1 (Microsoft Financials Database #1)

Examples of instance naming that do not meet the requirement:

database1, MyDatabase, SQL7

Interview the DBA to get an understanding of the naming scheme used to determine if the names are clear differentiations.

Fix:

Follow instructions for renaming a database instance:

SQL Server 7 – http://msdn.microsoft.com/en-us/library/aa197071.aspx

SQL Server 2000 – http://msdn.microsoft.com/en-us/library/aa197071.aspx

SQL Server 2005 – Review the sp_dropserver and sp_addserver procedures

Set the value so that it does not identify the SQL Server version and clearly identifies its purpose.

VKEY: V0015622	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0104: CAT III) The DBA will ensure all local and network-advertised named database services are uniquely and clearly identified.			

4.65 DG0106: Database data encryption configuration

Description: Authorizations may not sufficiently protect access to sensitive data and may require encryption. In some cases, the required encryption may be provided by the application accessing the database. In others, the DBMS may be configured to provide the data encryption. When the DBMS provides the encryption, the requirement must be implemented as identified by the Information Owner to prevent unauthorized disclosure or access.

Check:

Review the System Security Plan and AIS Functional Architecture documentation and note sensitive data identified by the Information Owner as requiring encryption using DBMS features administered by the DBA.

If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

Review the encryption configuration against the System Security Plan and AIS Functional Architecture documentation specification.

If the specified encryption is not configured, this is a Finding.

Fix:

Configure DBMS encryption features and functions as required by the System Security Plan and AIS Functional Architecture documentation. Discrepancies between what features are and are not available should be resolved with the Information Owner, Application Developer and DBA as overseen by the IAO.

VKEY: V0015143	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.3			
STIG Requirement:	(DG0106: CAT II) The DBA will ensure security requirements specific to the use of the database are configured as identified in the System Security Plan.			

4.66 DG0107: DBMS sensitive data identification

Description: A DBMS that does not have the correct confidentiality level identified or any confidentiality level assigned stands the chance of not being secured at a level appropriate to the risk it poses.

Check:

Review the System Security Plan and AIS Functional Architecture documentation for the DBMS and note any sensitive data that is identified.

Review database table column data or descriptions that indicate sensitive data. For example, a data column labeled "SSN" could indicate social security numbers are stored in the column. Question the IAO or DBA where any questions arise.

General categories of sensitive data requiring identification include any personal identifiable information (PII) involving health, financial and security proprietary or sensitive business data or data that might be classified.

If any columns in the database contain data considered sensitive and is not referenced in the System Security Plan and AIS Functional Architecture documentation, this is a Finding.

Fix:

Include identification of any sensitive data in the System Security Plan and AIS Functional Architecture. Include discussions of data that appear to be sensitive and annotate why it is not marked as such.

VKEY: V0015144	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.4.4			
STIG Requirement:	(DG0107: CAT II) The IAO will ensure all categories of sensitive data stored or processed by the database are identified in the AIS functional architecture documentation.			

4.67 DG0108: DBMS restoration priority

Description: When DBMS service is disrupted, the impact it has on the overall mission of the organization can be severe. Without the proper assignment of the priority to be placed on restoration of the DBMS and its subsystems, restoration of DBMS services may not meet mission requirements.

Check:

Review the System Security Plan to discover the restoration priority assigned to the DBMS. If it is not assigned, this is a Finding.

Fix:

Review the mission criticality of the DBMS in relation to the overall mission of the organization and assign it a restoration priority.

VKEY: V0015145	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.4.5			
STIG Requirement:	(DG0108: CAT III) The IAO will ensure the restoration priority of the database and its supporting subsystems are identified in the System Security Plan.			

4.68 DG0109: DBMS dedicated host

Description: In the same way that added security layers can provide a cumulative positive effect on security posture, multiple applications can provide a cumulative negative effect. A vulnerability and subsequent exploit to one application can lead to an exploit of other applications sharing the same security context. For example, an exploit to a web server process that leads to unauthorized administrative access to the host system can most likely lead to a compromise of all applications hosted by the same system. A DBMS not installed on a dedicated host may pose a threat to and be threatened by other hosted applications. Applications that share a single DBMS may also create risk to one another. Access controls defined for one application by default may provide access to the other application's database objects or directories. Any method that provides any level of separation of security context assists in the protection between applications.

Check:

Review the list of processes/services running on the DBMS host system.

For Windows, review the Services snap-in. Investigate with the DBA/SA any unknown services.

If any of the services or processes are identified as supporting applications or functions not authorized in the System Security Plan, this is a Finding.

Note: Only applications that are operationally required to share the same host system may be authorized to do so. Applications that share the same host for administrative, financial or other non-operational reasons may not be authorized and are a Finding.

Fix:

A dedicated host system in this case refers to an instance of the operating system at a minimum. The operating system may reside on a virtual host machine if supported by the DBMS vendor.

Remove any unauthorized processes or services and install on a separate host system. Where separation is not supported, update the System Security Plan and provide the technical requirement for having the application share a host with the DBMS.

VKEY: V0015146	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP
IA Control: DCPA	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.6			
STIG Requirement:	(DG0109: CAT II) The IAO will ensure the DBMS host is dedicated to support of the DBMS and is not shared with other application services including web, application, file, print, or other services unless mission or operationally required and documented in the System Security Plan.			

4.69 DG0110: DBMS host shared with a security service

Description: The Security Support Structure is a security control function or service provided by an external system or application. An example of this would be a Windows domain controller that provides identification and authentication that can be used by other systems to control access. The vulnerabilities and, therefore, associated risk of a DBMS installed on a system that provides a security support structure is significantly higher than when installed with other functions that do not provide security support. In cases where the DBMS is dedicated to local support of a security support function (e.g. a directory service), separation may not be possible.

Check:

Review the services and processes active on the DBMS host system.

If the host system is acting as a Windows domain controller, this is a finding.

If the host system is supporting any other directory or security service that does not use the DBMS to store the directory information, this is a Finding.

Note: A local installation of Anti-virus or Firewall does not constitute a security service in this context.

Fix:

Either move the DBMS installation to a dedicated host system or move the directory or security services to another host system.

A dedicated host system in this case refers to an instance of the operating system at a minimum. The operating system may reside on a virtual host machine if supported by the DBMS vendor.

VKEY: V0015179	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP
IA Control: DCSP	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.11			
STIG Requirement:	(DG0110: CAT II) The IAO will ensure the DBMS is not installed on a host system that provides directory services or other security services except when serving as a required component of the security service.			

4.70 DG0111: DBMS dedicated software directory and partition

Description: Protection of DBMS data, transaction and audit data files stored by the host operating system is dependent on OS controls. When different applications share the same database process, resource contention and differing security controls may be required to isolate and protect one application's data and audit logs from another. DBMS software libraries and configuration files also require differing access control lists.

Check:

Review the disk/directory specification where program files are stored:

For SQL Server 7 & 2000:

In the references below, replace **SQLRoot** with the registry path:

"HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer"

Review the disk/directory specification in the registry where program files are stored:

SQLRoot \ MSSQLServer \ Setup \ SQLPath

Review the default data and log directory specifications in the registry:

SQLRoot \ MSSQLServer \ DefaultData
SQLRoot \ MSSQLServer \ DefaultLog

For SQL Server 2005:

In the references below, replace **SQL5Root** with the registry path:

"HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server"

Replace **[#]** with the SQL Server instance number as listed under:

SQL5Root \ Instance Names \ SQL \ [instance name]

Review the disk/directory specification in the registry where program files are stored:

SQL5Root \ MSSQL.**[#]** \ Setup \ SQLProgramDir

Review the default data and log directory specifications in the registry:

SQL5Root \ MSSQL.**[#]** \ MSSQLServer \ DefaultData
SQL5Root \ MSSQL.**[#]** \ MSSQLServer \ DefaultLog

If the program file directory and disk partition is the same as either the DefaultData or the DefaultLog directories, this is a Finding.

Fix:

Configure the DBMS to specify dedicated host system disk directories to store database and log files for each application sharing the database. Do not share the application's data disk directory with application software libraries.

VKEY: V0015147	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: DCPA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.6			
STIG Requirement:	(DG0111: CAT II) The DBA will install and maintain database data directories including transaction log and audit files in dedicated directories or disk partitions separate from software or other application files.			

4.71 DG0114: Critical DBMS files fault protection

Description: DBMS recovery can be adversely affected by hardware storage failure. Impediments to DBMS recovery can have a significant impact on operations.

Check:

Interview the System Administrator to determine if Failover Clustering is employed on the DBMS host and that SQL Server is using Failover Clustering.

If the SQL Server instance employs Failover Clustering, this check is Not a Finding.

If the instance employs other high-availability redundancy host or DBMS clustering, this check is Not a Finding.

Failover clustering requires configuration of Microsoft Cluster Services (MSCS) to be running on the host (if available). View Services on the host to verify the service is active. Further, verify the Failover Cluster configuration by confirming that the MSCS service account has SYSADMIN privileges in the SQL Server instance.

Review the file and disk storage specification for the SQL Server databases.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

```
USE [database name]
SELECT filename
FROM sysfiles
WHERE status &0x40 = 0x40
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

```
USE [database name]
SELECT physical_name
FROM sys.database_files
WHERE type_desc = 'LOG'
```

Review the host disk system configuration.

1. Start / Administrative Tools / Computer Management
2. Expand Storage
3. Select Disk Management

If the Layout column for the identified volume does not display type "mirror" or "RAID-5", this is a Finding.

Fix:

Place SQL Server critical files including data, transaction and audit log files on fault-tolerant storage devices or employ SQL Server DBMS or OS clustering where supported by the DBMS.

VKEY: V0015119	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: COBR	Check Type: Verify	Database Level: False	Responsibility: SA/DBA	Documentable: False
Reference:	Database STIG 3.5.1			
STIG Requirement:	(DG0114: CAT II) The DBA will ensure files critical to database recovery are protected by employment of database and OS high-availability options such as storage on RAID devices.			

4.72 DG0115: DBMS trusted recovery

Description: A DBMS may be vulnerable to use of compromised data or other critical files at startup. Use of compromised files could introduce maliciously altered application code, relaxed security settings or loss of data integrity. Where available, DBMS mechanisms to ensure use of only trusted files can help protect the database from this type of compromise at DBMS startup.

Check:

Review DBMS configuration settings to see if mechanisms exist to specify use of only trusted files at DBMS startup.

If mechanisms do not exist, this check is Not a Finding.

If mechanisms do exist, review the configuration settings to determine if they have been employed properly.

An example for this would be the requirement for setting a shared password or a checksum validation, etc. If the mechanism is not employed or employed sufficiently, this is a Finding.

Fix:

Configure DBMS options available to ensure use of trusted data and other critical DBMS files where available.

VKEY: V0015625	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: COTR	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.5.5			
STIG Requirement:	(DG0115: CAT II) The DBA will configure the DBMS to use only authorized software, data files, or other critical files during recovery.			

4.73 DG0116: DBMS privileged role assignments

Description: Roles assigned privileges to perform DDL and/or system configuration actions in the database can lead to compromise of any data in the database as well as operation of the DBMS itself. Restrict assignment of privileged roles to authorized personnel and database accounts to help prevent unauthorized activity.

Check:

View SYSADMIN group membership:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.syslogins
WHERE sid <> 0x01
AND sysadmin = 1
ORDER BY name
```

For SQL Server 2005:

From the query prompt:

```
SELECT p.name
FROM [master].sys.server_principals p, [master].sys.server_role_members m
WHERE p.principal_id = m.member_principal_id
AND m.member_principal_id <> 1
AND m.role_principal_id = 3
ORDER BY p.name
```

Verify with the DBA that all users listed under System Administrators are authorized DBAs and authorized to manage the database system audit configuration. Authorized application object owner accounts are Not a Finding unless they are not disabled (DG0004). If any authorized application object owner accounts are enabled, this is a Finding (for DG0116).

If this is a production environment, verify with the DBA that none of the users listed under the SYSADMIN fixed server role are application administrators.

If the BUILTIN/Administrators group is listed as a member of the SYSADMIN fixed server role, this is a Finding.

Note: Removing BUILTIN/Administrators without creating an appropriate group to administer SQL Server will result in a ‘lock out’ condition within SQL Server. Ensure the proper steps have been taken to create a new group that is added to

SYSADMIN fixed server role before removing BUILTIN/Administrators. Also, ensure the SA password is known before making this change.

Fix:

Document IAO-authorized privileged role assignments in the System Security Plan. Remove assignments where not authorized.

If BUILTIN\Administrators is part of the SYSADMIN fixed server role, create a custom group for SYSADMIN functions, add authorized users to the custom group, add the group to the SYSADMIN fixed server role, remove BUILTIN\Administrators from the role. If other unauthorized users exist, remove them from the role.

To remove BUILTIN\Administrators from the SYSADMIN fixed server role:

1. Create a custom group for SYSADMIN functions
2. Add authorized users to the custom group
3. Add the group to the SYSADMIN fixed server role
4. Remove BUILTIN\Administrators from the role

VKEY: V0015626	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.11.2			
STIG Requirement:	(DG0116: CAT II) The IAO will ensure database privileged role assignments are restricted to IAO-authorized accounts.			

4.74 DG0117: DBMS administrative privilege assignment

Description: Privileges granted outside the role of the administrative user job function are more likely to go unmanaged or without oversight for authorization. Maintenance of privileges using roles defined for discrete job functions offers improved oversight of administrative user privilege assignments and helps to protect against unauthorized privilege assignment.

Check:

Review administrative accounts for direct privilege assignment.

If any administrative privileges have been assigned directly to a database account, this is a Finding.

Fix:

Create roles for administrative function assignments. Assign the necessary privileges for the administrative function to a role.

Assign administrative roles to authorized administrative users.

Document administrative job functions, roles, and required permissions in the System Security Plan.

Maintain evidence of administrative role authorizations.

VKEY: V0015627	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECPA	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.14			
STIG Requirement:	(DG0117: CAT II) The IAO will ensure all database administrative privileges defined within the DBMS and externally to the database are assigned using DBMS or OS roles.			

4.75 DG0118: IAM review of change in DBA assignments

Description: Unauthorized assignment of DBA privileges can lead to a compromise of DBMS integrity. Providing oversight to the authorization and assignment of privileges provides the separation of duty to support sufficient oversight.

Check:

Review the policy, procedures and implementation evidence for monitoring changes to DBA role assignments and procedures for notifying the IAM of the changes for review.

If policy, procedures and implementation evidence do not exist, this is a Finding.

Fix:

Develop, document and implement policy and procedures to monitor changes to DBA role assignments.

Develop, document and implement policy and procedures to notify the IAM of changes to DBA role assignments.

Include methods in the procedures that provide evidence of monitoring and notification.

VKEY: V0015127	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECPA	Check Type: Manual	Database Level: False	Responsibility: IAM	Documentable: False
Reference:	Database STIG 3.3.14			
STIG Requirement:	(DG0118: CAT II) The IAM will review DBA role assignments whenever changes to the assignments occur.			

4.76 DG0119: DBMS application user role privileges

Description: DBMS privileges to issue other than Database Manipulation Language (DML) commands provide means to affect database object configuration and use of resources. Application users do not require these privileges to complete non-administrative job functions. Where applications require administrative privileges to execute non-administrative functions, exploits of the application can lead to unauthorized administrative access to the DBMS.

Check:

Review privileges assigned to application user roles in the database.

If any privileges other than SELECT, UPDATE, DELETE or EXECUTE are assigned to application user roles, this is a Finding.

Fix:

Revoke administrative privileges from application user roles.

Do not allow Database Definition Language (DDL) or other administrative privileges for operation of the application, for example, do not create and drop database objects for temporary storage of data.

Consider, instead, the storage of temporary data in static database tables.

VKEY: V0015628	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0119: CAT II) The DBA will ensure database application user roles are restricted to select, insert, update, delete, and execute privileges.			

4.77 DG0120: DBMS application user access to external objects

Description: Access to objects stored and/or executed outside of the DBMS security context may provide an avenue of attack to host system resources not controlled by the DBMS. Any access to external resources from the DBMS can lead to a compromise of the host system or its resources.

Check:

View access permissions granted to external stored procedures:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object', p.action 'Action'
FROM sysprotects p, sysobjects o, sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND o.type = 'X'
ORDER BY u.name, o.name
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT DISTINCT u.name 'User', o.name 'Object', p.permission_name
'Action'
```

```
FROM sys.all_objects o, sys.database_principals u, sys.database_permissions
p
WHERE p.grantee_principal_id = u.principal_id
AND o.object_id = p.major_id
AND o.type = 'X'
ORDER BY u.name, o.name
```

User = NULL is a permission assignment to PUBLIC

If no results are listed, this is Not a Finding.

Results listed with User = NULL is a Finding (permissions assigned to PUBLIC).

Review results returned to named user/our group names. If any names returned are not listed as authorized in the System Security Plan, this is a Finding.

Fix:

Evaluate the associated risk in allowing access to external objects.

Consider the security context under which the object is accessed or whether the privileges required to access the object are available for assignment based on job function.

Where feasible, modify the application to use only objects stored internally to the database. Where not feasible, note the risk assessment and acceptance in the System Security Plan for access to external objects.

VKEY: V0015105	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0120: CAT II) The DBA will ensure database application user roles are not granted unauthorized access to external database objects.			

4.78 DG0123: DBMS Administrative data access

Description: Administrative data includes DBMS metadata and other configuration and management data. Unauthorized access to this data could result in unauthorized changes to database objects, access controls or DBMS configuration.

Check:

Review access controls on system tables.

Review access to configuration data stored in the database.

If any users not assigned DBA privileges are assigned access to the underlying tables, this is a Finding.

Fix:

Revoke access to system tables to non-DBA users.

Where use of system data is required by non-DBA users, provide controlled access for authorized functions via views, procedures, or other use of controlled objects.

VKEY: V0015631	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAN	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0123: CAT II) The DBA will ensure all access to sensitive application data stored inside the database, and in external host files, is granted only to database accounts and OS accounts in accordance with user functions as specified by the Information Owner.			

4.79 DG0124: DBA account use

Description: Use of privileged accounts for non-administrative purposes puts data at risk of unintended or unauthorized loss, modification or exposure. In particular, DBA accounts if used for non-administration application development or application maintenance can lead to miss-assignment of privileges where privileges are inherited by object owners. It may also lead to loss or compromise of application data where the elevated privileges bypass controls designed in and provided by applications.

Check:

Review accounts assigned fixed server roles and fixed database roles with the DBA/IAO and as documented in the System Security Plan.

Review other database or application roles assigned to the accounts assigned fixed roles as documented in the System Security Plan.

If any accounts assigned fixed roles are also assigned application roles or other application object privilege roles or own application objects used for other than DBA functions, this is a Finding.

Fix:

Create separate accounts for administration activities.

Develop, document and implement policy and procedures that require separate, unprivileged or less-privileged accounts for development, testing and application users.

VKEY: V0015632	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0124: CAT II) The IAO will ensure privileged database accounts are used only for privileged database job functions. The IAO will ensure non-privileged database accounts are used to perform non-privileged job functions.			

4.80 DG0125: DBMS account password expiration

Description: Unchanged passwords provide a means for compromised passwords to be used for unauthorized access to DBMS accounts over a long time.

Check:

If no DBMS accounts authenticate using passwords, this check is Not a Finding.

If DBMS uses Windows Authentication only, this check is Not a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.sql_logins
WHERE type = 'S'
AND is_expiration_checked <> '1'
ORDER BY name
```

If any names are returned, this is a Finding.

Fix:

Set SQL Server logins to check password expiration.

For SQL Server 2005:

```
ALTER LOGIN [user name] WITH CHECK_EXPIRATION = ON
```

VKEY: V0015153	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: IAIA	Check Type: Auto	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2.2			
STIG Requirement:	(DG0125: CAT II) The DBA will set expiration times for interactive database user account passwords to 60 days or less where supported by the DBMS.			

4.81 DG0127: DBMS account password easily guessed

Description: DBMS account passwords set to common dictionary words or values render accounts vulnerable to password guessing attacks and possible unauthorized access.

Check:

If no DBMS accounts authenticate using passwords, this check is Not a Finding.

If DBMS uses Windows Authentication only, this check is Not a Finding.

Review methods for protecting accounts from assignment of easily guessed passwords. If methods do not include at least one of the following or a viable alternate means to prevent use of easily guessed passwords, this is a Finding.

1. Password cracker run frequently to report easily guessed passwords
2. Automated routine to check passwords against password dictionaries at password assignment time
3. User training and understanding of the risk of easily guessed passwords
4. Using Windows Authentication for database accounts

Fix:

Employ preventative means, user training and/or password cracking routines to discover and prevent easily guessed passwords in the database.

VKEY: V0015634	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2.2			
STIG Requirement:	(DG0127: CAT II) The DBA will configure or test database account passwords to prevent use of easily guessed or discovered values.			

4.82 DG0128: DBMS default passwords

Description: By default, the sa account password is blank. If the sa account is left without password protection, anyone can act as administrator on the SQL server. Once an authorized user gains access to the sa account, it is easy to gain access to admin privileges on the Windows NT Server by using commands such as xp_cmdshell.

Check:

Note: This check assumes you are using Windows authentication for SQL Server. It lists the SQL Server login accounts not directly tied to a local or domain Windows account.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT s.name
FROM [master].dbo.syslogins s, [master].dbo.sysusers u
WHERE s.sid = u.sid
AND u.issqluser = 1
```

Confirm any accounts listed do not have default or NULL passwords assigned. If any do, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name FROM [master].sys.sql_logins
WHERE type = 'S'
```

Confirm any accounts listed do not have default or NULL passwords assigned. If any do, this is a Finding.

Fix:

Assign a password to accounts that meet DoD complexity requirements.

From the query prompt:

```
USE master
ALTER LOGIN [name] WITH PASSWORD = '[new password]'
```

Replace [new password] with a password and [name] with the account name.

Use the SQL Server Enterprise Manager GUI to change the assigned password of any SQL Server–related service. Each service must be changed individually.

VKEY: V0015635	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2.2			
STIG Requirement:	(DG0128: CAT I) The DBA will assign custom passwords to all default database accounts whether created by the installation of the database software or database components or by third-party applications.			

4.83 DG0130: DBMS passwords in executables

Description: The storage of passwords in application or job code prevents compliance with password expiration and other management requirements as well as provides another means for potential discovery. If the password is not encrypted within the code or job, then it is easily accessible for any account with read access to the executable file. If it is encrypted, it still may be vulnerable to possible decryption efforts that may easily go undetected.

Check:

Review accounts used by applications or batch jobs to access the database.

Ask the DBA and/or IAO to determine if the jobs or executables use passwords for authentication.

If any do not use passwords for authentication, this check is Not a Finding.

If any do use passwords for authentication, ask where the password is stored for access by the job or executable.

If the password is stored in the batch script or executable code, this is a Finding.

Fix:

Design DBMS jobs and applications to store and manage passwords in external files or objects protected with FIPS 140-2 encryption.

Consider alternatives to password authentication for batch jobs and executables.

VKEY: V0015637	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Interview	Database Level: False	Responsibility: DBA/IAO	Documentable: False
Reference:	Database STIG 3.2.2.1			
STIG Requirement:	(DG0130: CAT II) The DBA/IAO will ensure database account passwords are not stored in batch jobs or application source code.			

4.84 DG0131: DBMS default account names

Description: The 'sa' account is a well-known account. Well-known account names provide an easier target for attack. Renaming the sa account helps reduce the risk of an attack to this built-in account.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.sql_logins
WHERE name = 'sa'
```

If the value returned for Name is 'sa', this is a Finding.

Fix:

For SQL Server 2005:

From the query prompt:

```
ALTER LOGIN sa WITH NAME = '[new sa name]'
```

Replace [new sa name] with a custom-supplied name

VKEY: V0015638	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Auto	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2			
STIG Requirement:	(DG0131: CAT III) The DBA will change or delete default account usernames where supported.			

4.85 DG0133: DBMS Account lock time

Description: When no limit is imposed on failed logon attempts and accounts are not disabled after a set number of failed access attempts, the DBMS account becomes vulnerable to sustained attacks. When access attempts continue unrestricted, the likelihood of success is increased. A successful attempt can result in unauthorized access to the database.

Check:

If the DBMS does not provide a method or means for configuration of account lock times, this check is Not a Finding.

Review the account lock time configuration setting. If the lock time is not set to unlimited or is set to allow the DBMS to unlock the account after a pre-determined amount of time, this is a Finding.

For DBMS accounts using Windows Authentication:

1. Launch the Group Policy Editor on the DBMS Server
2. Under Computer Configuration:
    a. Expand Windows Settings
    b. Expand Security Settings
    c. Expand Account Policies
    d. Select Account Lockout Policy
3. Review Account Lockout Duration, Account Lockout Threshold and Reset Account Lockout Counter After policies

If Account Lockout Duration is not set or set to a value greater than 0, this is a Finding.

If Account Lockout Threshold is not set or set to a value greater than 3, this is a Finding.

If Reset Account Lockout Counter After is not set to its maximum value (For Windows 2003, this is 99999), this is a Finding.

Fix:

Configure the database to maintain an account lock time until the account is manually unlocked by an authorized account administrator.

For DBMS accounts using Windows Authentication:

1. Launch the Group Policy Editor on the DBMS Server
2. Under Computer Configuration:
    a. Expand Windows Settings
    b. Expand Security Settings

c. Expand Account Policies
d. Select Account Lockout Policy

3. Set "Account Lockout Threshold" = 3
4. Set or Reset "Account Lockout Duration" = 0
5. Set or Reset "Reset Account Lockout Counter After" = 99999 (about 69 days, which is max for this policy setting)
6. Close Group Policy Editor

Document these settings in the System Security Plan

VKEY: V0015639	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLO	Check Type: Manual	Database Level: False	Responsibility: DBA/SA	Documentable: False
Reference:	Database STIG 3.3.10			
STIG Requirement:	(DG0133: CAT II) The DBA will configure the DBMS to set the duration of database account lockouts to an unlimited time that requires the DBA to manually unlock the account.			

4.86 DG0140: DBMS security data access

Description: DBMS security data is useful to malicious users to perpetrate activities that compromise DBMS operations or data integrity. Auditing of access to this data supports forensic and accountability investigations.

Check:

Note: Checks DM0510 and DG0029/DG0145/DM5267 cover auditing of data within SQL Server and should not be included in this check.

Determine locations of DBMS audit, configuration, credential and other security data.

Review audit settings for these files or data objects. If the security data is not audited for access, consider the operational impact and appropriateness for access that is not audited.

If the risk for incomplete auditing of the security files is reasonable and documented in the System Security Plan, do not include this as a Finding.

Fix:

Determine all locations for storage of DBMS security and configuration data. Enable auditing for access to any security data where supported by the DBMS.

If audit for access results in an unacceptable adverse impact on application operation, scale back the audit to a reasonable and acceptable level.

Document any incomplete audit with acceptance of the risk of incomplete audit in the System Security Plan.

VKEY: V0015643	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAR	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.2			
STIG Requirement:	(DG0140: CAT II) The DBA will ensure all access to DBMS configuration files, database audit data, database credential, or any other DBMS security information is audited.			

4.87 DG0141: DBMS access control bypass

Description: Detection of suspicious activity including access attempts and successful access from unexpected places, during unexpected times, or other unusual indicators can support decisions to apply countermeasures to deter an attack. Without detection, malicious activity may proceed without impedance.

Check:

From the query prompt:

EXEC XP_LOGINCONFIG 'audit level'

If the config_value returned is not 'All' or 'Failure', this is a finding.

Fix:

Enable Auditing level.

For SQL Server 7 & 2000:

From the SQL Server Enterprise Manager GUI:

1. Navigate to the SQL Server instance name
2. Right-click on it
3. Select Properties
4. Select Security tab or page
5. Review Security/Audit level
6. Select All or Failure from the Audit Level selection
7. Apply changes
8. Exit the SQL Server Enterprise Manager GUI

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Navigate to the SQL Server instance name
2. Right-click on it
3. Select Properties
4. Select Security tab or page
5. Review Login Auditing selection
6. Select "Failed logins only" or "Both failed and successful logins" from the Login Auditing section
7. Apply changes
8. Exit the SQL Server Management Studio GUI

VKEY: V0015644	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAR	Check Type: Auto	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.2			
STIG Requirement:	(DG0141: CAT II) The DBA will ensure all database logons, account locking events, blocking or disabling of a database account or logon source location, or any attempt to circumvent access controls is audited.			

4.88 DG0142: DBMS privileged action audit

Description: The default audit trace provides a log of activity and changes primarily related to DBMS configuration options. While the other required audit options may include audits of the same or similar events, this option provides a standard audit trail provided by the vendor that can provide consistent results across systems. If audit record generation overwhelms system resources and it is determined that this requirement is unnecessarily redundant, the IAO may authorize the disabling of this setting.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'default trace enabled'
```

If the value of Config_Value is 1, this is Not a Finding.

If the value of Config_Value is 0, confirm in the System Security Plan and AIS Functional Architecture documentation that this option is documented and is not required and approved by the IAO. If it is not documented and is required and approved, this is a Finding.

Fix:

For SQL Server 2005:

Authorize and document requirements for use of the default trace option in the System Security Plan and AIS Functional Architecture documentation. Where authorized, enable its use.

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'default trace enabled', 1
RECONFIGURE
```

VKEY: V0015645	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAR	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.2			
STIG Requirement:	(DG0142: CAT II) The DBA will ensure privileged DBMS actions and changes to security labels or sensitivity markings of data in the DBMS are audited.			

4.89 DG0145: DBMS audit record content

Description: SQL Server Trace provides the ability to audit security related activities as they occur within the server. A secure system requires auditing of events in order to detect possible attacks on the server and to reconstruct events in cases where security violations have been found. For auditing to work effectively, it must be properly configured to audit the appropriate events and return the necessary data about those events. SQL Server Trace Events are organized into category classes. Events that pertain to security are in the Security Audit class. At a minimum, you should consider auditing some or all of these events in order to maintain a secure system.

Check:

If C2 Auditing is enabled (See Check DM0510**:** C2 audit mode), this check is Not a Finding.

Determine the SQL Server Edition:

From the query prompt:

```
SELECT CONVERT(INT, SERVERPROPERTY('EngineEdition'))
```

If value returned is 1 (Personal or Desktop Edition) or 4 (Express Edition), if auditing is not enabled or not configured completely to requirements, review the System Security Plan. If this is properly explained in the System Security Plan, this is Not a Finding. If this is not documented or documented poorly in the System Security Plan, this is a Finding.

If value returned is 2 (Standard Edition) or 3 (Enterprise/Developer Edition), findings in all steps apply.

For SQL Server 2000 & 2005:

Note: Complete all checks to determine final Finding results.

1. Check to see that all required events are being audited

For SQL Server 2000:

From the query prompt:

```
SELECT DISTINCT traceid FROM ::FN_TRACE_GETINFO('0')
```

For SQL Server 2005:

From the query prompt:

SELECT DISTINCT traceid FROM ::FN_TRACE_GETINFO('0')
WHERE traceid <> 1 – Omit the default trace in SQL Server 2005

All currently defined traces for the SQL server instance will be listed. If no traces are returned, this is a Finding.

2. For each traceid listed, replacing # with a traceid

From the query prompt:

SELECT DISTINCT(eventid) FROM ::FN_TRACE_GETEVENTINFO('#')

For SQL Server 2000, the required eventid's 18, 20, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 115,116,117, and 118 should be listed.

For SQL Server 2005, the following additional eventid's should be listed:
14, 15, 128, 129, 130, 131, 132, 133, 134, 135, 152, 153, 170, 171, 172, 173, 175, 176, 177, 178

If any of the audit events or eventid's required above are not listed, this is a Finding.

3. Check to see that auditing is set to shutdown the database system if auditing fails (For each traceid listed, replacing # with a traceid)

For SQL Server 2000 & 2005:

From the query prompt:

SELECT CAST(value AS INT) FROM ::FN_TRACE_GETINFO('#')
WHERE property = 1 AND value = 4

If value returned is not equal to 4 for any traceid, this is a Finding.

Fix:

For SQL Server 2000 & 2005:

Create and start an audit trace that audits required events.

Note: Additional audit events are required for SQL Server 2005 and are included in the procedure below. Remove these for a SQL Server 2000 instance where marked.

CREATE PROCEDURE my_audit AS

-- Create a Queue

```
DECLARE @rc INT
DECLARE @TraceID INT
DECLARE @maxfilesize BIGINT
DECLARE @my_audit_log NVARCHAR(128)
SET @maxfilesize = 5

-- Define custom @my_audit_log to path\filename
SET @my_audit_log = 'd:\sqlserver\audit\myauditlog.log'

EXEC @rc = SP_TRACE_CREATE @TraceID output, 6, @my_audit_log,
@maxfilesize, NULL
IF (@rc != 0) GOTO Error

-- Client side File and Table cannot be scripted.
-- Set the events:
DECLARE @on BIT
SET @on = 1

-- Logins are audited based on SQL Server instance
-- setting Audit Level stored in registry
-- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL
Server\MSSQL.[#]\MSSQLServer\AuditLevel

-- Audit Login System Starts/Stops
EXEC SP_TRACE_SETEVENT @TraceID, 18, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 18, 41, @on

-- Audit Login Failed
EXEC SP_TRACE_SETEVENT @TraceID, 20, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 28, @on
```

```
EXEC SP_TRACE_SETEVENT @TraceID, 20, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 20, 41, @on

-- Audit Database Grant, Deny, Revoke event
EXEC SP_TRACE_SETEVENT @TraceID, 102, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 102, 41, @on

-- Audit Schema Object Grant, Deny, Revoke event
EXEC SP_TRACE_SETEVENT @TraceID, 103, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 103, 41, @on

-- Audit Login Change Property Event
EXEC SP_TRACE_SETEVENT @TraceID, 104, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 104, 41, @on

-- Audit Login Grant, Deny, Revoke
EXEC SP_TRACE_SETEVENT @TraceID, 105, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 12, @on
```

```
EXEC SP_TRACE_SETEVENT @TraceID, 105, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 105, 41, @on

-- Audit Login Change Property Event
EXEC SP_TRACE_SETEVENT @TraceID, 106, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 106, 41, @on

-- Audit Login Change Password Event
EXEC SP_TRACE_SETEVENT @TraceID, 107, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 107, 41, @on

-- Audit Add Login to Server Role Event
EXEC SP_TRACE_SETEVENT @TraceID, 108, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 108, 35, @on
```

```
EXEC SP_TRACE_SETEVENT @TraceID, 108, 41, @on

-- Audit Add Database User Event
EXEC SP_TRACE_SETEVENT @TraceID, 109, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 109, 41, @on

-- Audit Add Member to DB Role Event
EXEC SP_TRACE_SETEVENT @TraceID, 110, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 110, 41, @on

-- Audit Add/Drop Role Event
EXEC SP_TRACE_SETEVENT @TraceID, 111, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 111, 41, @on

-- Audit App Role Change Password Event
EXEC SP_TRACE_SETEVENT @TraceID, 112, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 14, @on
```

```
EXEC SP_TRACE_SETEVENT @TraceID, 112, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 112, 41, @on

-- Audit use of Statement Permission (such as CREATE TABLE)
EXEC SP_TRACE_SETEVENT @TraceID, 113, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 113, 41, @on

-- Audit Backup/Restore Event
EXEC SP_TRACE_SETEVENT @TraceID, 115, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 115, 41, @on

-- Audit Change Audit Event
EXEC SP_TRACE_SETEVENT @TraceID, 117, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 117, 41, @on
```

```
-- Audit Object Derived Permission Event (CREATE, ALTER, DROP)
EXEC SP_TRACE_SETEVENT @TraceID, 118, 10, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 11, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 12, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 14, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 15, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 21, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 22, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 23, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 28, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 35, @on
EXEC SP_TRACE_SETEVENT @TraceID, 118, 41, @on

--------------------------------------------------
-- The following are for SQL Server 2005 only
-- Remove remaining setevent statements for
-- Versions earlier than 2005
--------------------------------------------------

-- Audit Database Management Event
EXEC SP_TRACE_SETEVENT @TraceID, 128, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 128, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 128, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 128, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 128, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 128, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 128, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 128, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 128, 64, @on --
SessionLoginName

-- Audit Database Object Management Event
EXEC SP_TRACE_SETEVENT @TraceID, 129, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 129, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 129, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 129, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 129, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 129, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 129, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 129, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 129, 64, @on --
SessionLoginName

-- Audit Database Principal Management Event
EXEC SP_TRACE_SETEVENT @TraceID, 130, 1, @on -- TextData
```

```
EXEC SP_TRACE_SETEVENT @TraceID, 130, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 130, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 130, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 130, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 130, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 130, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 130, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 130, 64, @on --
SessionLoginName

-- Audit Schema Object Management Event
EXEC SP_TRACE_SETEVENT @TraceID, 131, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 131, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 131, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 131, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 131, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 131, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 131, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 131, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 131, 59, @on -- ParentName
EXEC SP_TRACE_SETEVENT @TraceID, 131, 64, @on --
SessionLoginName

-- Audit Server Principal Impersonation Event
EXEC SP_TRACE_SETEVENT @TraceID, 132, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 132, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 132, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 132, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 132, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 132, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 132, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 132, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 132, 64, @on --
SessionLoginName

-- Audit Database Principal Impersonation Event
EXEC SP_TRACE_SETEVENT @TraceID, 133, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 133, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 133, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 133, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 133, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 133, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 133, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 133, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 133, 64, @on --
SessionLoginName
```

```
-- Audit Server Object Take Ownership Event
EXEC SP_TRACE_SETEVENT @TraceID, 134, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 134, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 134, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 134, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 134, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 134, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 134, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 134, 64, @on --
SessionLoginName

-- Audit Database Object Take Ownership Event
EXEC SP_TRACE_SETEVENT @TraceID, 135, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 135, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 135, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 135, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 135, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 135, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 135, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 135, 64, @on --
SessionLoginName

-- Audit Change Database Owner
EXEC SP_TRACE_SETEVENT @TraceID, 152, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 152, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 152, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 152, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 152, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 152, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 152, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 152, 64, @on --
SessionLoginName

-- Audit Schema Object Take Ownership Event
EXEC SP_TRACE_SETEVENT @TraceID, 153, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 153, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 153, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 153, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 153, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 153, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 153, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 153, 59, @on -- ParentName
EXEC SP_TRACE_SETEVENT @TraceID, 153, 64, @on --
SessionLoginName
```

```
-- Audit Server Scope GDR Event
EXEC SP_TRACE_SETEVENT @TraceID, 170, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 170, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 170, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 170, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 170, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 170, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 170, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 170, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 170, 64, @on --
SessionLoginName

-- Audit Server Object GDR Event
EXEC SP_TRACE_SETEVENT @TraceID, 171, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 171, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 171, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 171, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 171, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 171, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 171, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 171, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 171, 64, @on --
SessionLoginName

-- Audit Database Object GDR Event
EXEC SP_TRACE_SETEVENT @TraceID, 172, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 172, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 172, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 172, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 172, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 172, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 172, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 172, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 172, 64, @on --
SessionLoginName

-- Audit Server Operation Event
EXEC SP_TRACE_SETEVENT @TraceID, 173, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 173, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 173, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 173, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 173, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 173, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 173, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 173, 40, @on -- DBUserName
```

```
EXEC SP_TRACE_SETEVENT @TraceID, 173, 64, @on --
SessionLoginName

-- Audit Server Alter Trace Event
EXEC SP_TRACE_SETEVENT @TraceID, 175, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 175, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 175, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 175, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 175, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 175, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 175, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 175, 64, @on --
SessionLoginName

-- Audit Server Object Management Event
EXEC SP_TRACE_SETEVENT @TraceID, 176, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 176, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 176, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 176, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 176, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 176, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 176, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 176, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 176, 64, @on --
SessionLoginName

-- Audit Server Principal Management Event
EXEC SP_TRACE_SETEVENT @TraceID, 177, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 177, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 177, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 177, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 177, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 177, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 177, 35, @on -- DatabaseName
EXEC SP_TRACE_SETEVENT @TraceID, 177, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 177, 64, @on --
SessionLoginName

-- Audit Database Operation Event
EXEC SP_TRACE_SETEVENT @TraceID, 178, 1, @on -- TextData
EXEC SP_TRACE_SETEVENT @TraceID, 178, 11, @on -- LoginName
EXEC SP_TRACE_SETEVENT @TraceID, 178, 14, @on -- StartTime
EXEC SP_TRACE_SETEVENT @TraceID, 178, 21, @on -- EventSubClass
EXEC SP_TRACE_SETEVENT @TraceID, 178, 23, @on -- Success
EXEC SP_TRACE_SETEVENT @TraceID, 178, 34, @on -- ObjectName
EXEC SP_TRACE_SETEVENT @TraceID, 178, 35, @on -- DatabaseName
```

```
EXEC SP_TRACE_SETEVENT @TraceID, 178, 40, @on -- DBUserName
EXEC SP_TRACE_SETEVENT @TraceID, 178, 64, @on --
SessionLoginName

-------------------------------------------------
-- End SQL Server 2005 only audit events
-------------------------------------------------

-- Set the Filters.
DECLARE @intfilter INT
DECLARE @bigintfilter bigint

-- Set the trace status to start.
EXEC SP_TRACE_SETSTATUS @TraceID, 1

-- Display trace ID for future references.
SELECT TraceID = @TraceID
GOTO Finish

Error:
SELECT ErrorCode = @rc

Finish:
GO
EXEC SP_PROCOPTION 'my_audit', 'startup', 'true'
GO
```

Note: Replace ['d:\sqlserver\audit\myauditlog.log'] with the PATH and file name to your audit file

VKEY: V0015646	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAR	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.2			
STIG Requirement:	(DG0145: CAT II) The DBA will ensure audit records contain the user ID, date and time of the audited event, and the type of the event.			

4.90 DG0151: DBMS random port use

Description: Use of static, default ports helps management of enterprise network device security controls. Use of non-default ports makes tracking and protection of published vulnerabilities to services and protocols more difficult to track and block.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Port

If the value = 0, this is a Finding (Dynamic port assignment in use).

If the value = 2383, this is Not a Finding.

The Port value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[Port]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

If a different port is assigned, verify that the port reassignment requirement is documented and approved in the System Security Plan and AIS Functional Architecture documentation.

Fix:

Use static, default network ports.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Port
5. Set value = 2383 or IAO-approved value
6. Click OK

VKEY: V0015648	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCPP	Check Type: Manual	Database Level: False	Responsibility: SA / DBA	Documentable: False
Reference:	Database STIG 3.1.7			
STIG Requirement:	(DG0151: CAT II) The SA/DBA will ensure random port assignment to network connections is disabled when traversing network firewalls.			

4.91 DG0152: DBMS network port, protocol and services (PPS) use

Description: Non-standard network ports, protocol or services configuration or usage could lead to bypass of network perimeter security controls and protections.

Check:

For SQL Server 7 & 2000:

From the SQL Server Network Utility:

1. Select the instance name under review
2. View all enabled protocols
3. Select TCP/IP
4. Click Properties

OR

View the registry value:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ MSSQLServer \ MSSQLServer \ SuperSocketNetLib \ ProtocolList

If a protocol other than TCP is listed, this is a Finding.

View the registry value:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ MSSQLServer \ MSSQLServer \ SuperSocketNetLib \ Tcp \ TcpPort

If any value (including 0) is entered for TCP Dynamic Ports, this is a Finding.

A blank value indicates dynamic ports are not enabled and is Not a Finding.

For SQL Server 2005:

From the SQL Server Configuration Manager GUI:

1. Expand SQL Server 2005 Network Configuration
2. Select Protocols for [instance name]
3. Right-click on TCP/IP
4. Select Properties
5. Select IP Addresses tab

View all TCP Dynamic Ports and TCP Port values for all IP addresses.

OR

View the registry values:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ MSSQLServer \ SuperSocketNetLib \ Tcp\IP[#] \ TCPDynamicPorts

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ MSSQLServer \ SuperSocketNetLib \ Tcp\IP[#] \ TcpPort

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ MSSQLServer \ SuperSocketNetLib \ IPAll \ TCPDynamicPorts

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ MSSQLServer \ SuperSocketNetLib \ IPAll \ TcpPort

If any value (including 0) is entered for TCP Dynamic Ports, this is a Finding.

A blank value indicates dynamic ports are not enabled and is Not a Finding.

If the TCP Port value is set to 1433, 1434 or both, this is Not a Finding.

If any TCP Port value is set to a different port number, verify network traffic for the DBMS does not cross network or enclave boundaries as defined in the PPS CAL or registered with the PPS:

http://iase.disa.mil/ports/index.html

If any do and are not registered or allowed per the PPS, this is a Finding.

Fix:

Set TCP/IP ports to default values. Disable dynamic port usage.

For SQL Server 7 & 2000:

From the SQL Server Network Utility:

1. Select the instance name under review
2. View all enabled protocols
3. Select TCP/IP
4. Click Properties

Set the TCP Port values for ports accessed across a network boundary to 1433, or 1434.

For SQL Server 2005:

From the SQL Server Configuration Manager GUI:

1. Expand SQL Server 2005 Network Configuration
2. Select Protocols for [instance name]
3. Right-click on TCP/IP
4. Select Properties
5. Select IP Addresses tab
6. Clear any value listed in TCP Dynamic Ports for all IP addresses
7. Set all TCP Port values for ports accessed across a network boundary to 1433, 1434 or both

Ensure port is registered in the PPS CAL for use outside the enclave:

http://iase.disa.mil/ports/index.html

VKEY: V0015148	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCPP	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.7			
STIG Requirement:	(DG0152: CAT II) The SA/DBA will ensure DBMS network communications comply with DODI 8551.1 Ports, Protocols, and Services Management.			

4.92 DG0153: DBMS DBA roles assignment approval

Description: The DBA role and associated privileges provide complete control over the DBMS operation and integrity. DBA role assignment without authorization could lead to the assignment of these privileges to untrusted and untrustworthy persons and complete compromise of DBMS integrity.

Check:

Review the documented procedures for approval and granting of DBA privileges.

Review implementation evidence for the procedures.

If procedures do not exist or evidence that they are followed does not exist, this is a Finding.

Fix:

Develop, document and implement procedures to ensure all DBA role assignments are authorized and assigned by the IAO. Include methods that provide evidence of approval in the procedures.

VKEY: V0015149	Severity: CAT 3		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSD	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.9			
STIG Requirement:	(DG0153: CAT III) The IAO will assign and authorize DBA responsibilities for the DBMS.			

4.93 DG0154: DBMS System Security Plan

Description: A System Security Plan identifies security control applicability and configuration for the DBMS. It also contains security control documentation requirements. Security controls applicable to the DBMS may not be documented, tracked or followed if not identified in the System Security Plan. Any omission of security control consideration could lead to an exploit of DBMS vulnerabilities.

Check:

Review the System Security Plan for the DBMS with the IAO.

Review coverage of the following in the System Security Plan:

1. Technical, administrative and procedural IA program and policies that govern the DBMS
2. Identification of all IA personnel (IAM, IAO, DBA, SA) assigned responsibility to the DBMS
3. Specific IA requirements and objectives (e.g., requirements for data handling or dissemination (to include identification of sensitive data stored in the database, database application user job functions/roles and privileges), system redundancy and backup, or emergency response)

If the System Security Plan does not exist, this is a Finding.

If the System Security Plan does not include the information listed above at a minimum, this is a Finding.

Fix:

Develop, document and implement a System Security Plan for the DBMS or include IA documentation related to the DBMS in the System Security Plan of the system that the DBMS supports.

Refer to Section 3.4 in the Microsoft SQL Server Database Security Checklist for information on how to develop a System Security Plan.

Include or note additional information in the System Security Plan where required in other DBMS checks.

VKEY: V0015150	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSD	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.9			
STIG Requirement:	(DG0154: CAT III) The IAO will ensure the DBMS is included in or has defined for it a System Security Plan.			

4.94 DG0155: DBMS trusted startup

Description: The DBMS opens data files and reads configuration files at system startup. If the DBMS does not verify the trustworthiness of the files at startup, it is vulnerable to malicious alterations of its configuration or unauthorized replacement of data.

Check:

If the DBMS does not provide a means to ensure the trustworthiness of files at startup, this check is Not a Finding.

Review the configuration of the file verification at startup. The verification may be means of a trusted password set on the file or an alternate means.

If the DBMS is not configured to verify the files, this is a Finding.

Fix:

Configure the DBMS to use available means to test the validity of data and configuration files at DBMS startup.

VKEY: V0015649	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSS	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.12			
STIG Requirement:	(DG0155: CAT II) The DBA will ensure all applicable DBMS settings are configured to use trusted files, functions, features, or other components during startup, shutdown, aborts, or other unplanned interruptions.			

4.95 DG0157: DBMS remote administration

Description: The Dedicated Administrator Connection (DAC) option by default allows only local client connections to the database when other access is not available due to a malfunction or problem with database connections. The availability and use of remote administrative connections requires network traffic encryption and additional logging requirements. Disabling this feature helps to protect the database against malicious attacks against the privileged account.

Check:

For SQL Server 7 & 2000:

If the DBMS does not support remote DBMS administration, this check is Not Applicable.

If the DBMS supports remote DBMS administration, Review the System Security Plan for authorization, assignments and usage procedures.

If remote administration of the DBMS is not documented or poorly documented, this is a Finding.

If remote administration of the DBMS is not authorized and not disabled, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'remote admin connections'
```

If the value of Config_Value is 0, this is Not a Finding.

If the value of Config_Value is 1, confirm in the System Security Plan that remote admin connection access is required and approved by the IAO. If it is not documented, required and approved, this is a Finding.

Fix:

For SQL Server 7 & 2000:

Disable remote administration of the DBMS where not required.

Where remote administration of the DBMS is required, develop, document and implement policy and procedures on its use. Assign remote administration privileges to IAO-authorized personnel only.

Document in the System Security Plan

For SQL Server 2005:

Where remote admin connection access is part of the designed and approved use of the SQL Server database, document the requirement in the System Security Plan. Where remote admin connection access is not required, disable its use.

From the query prompt:

```
EXEC SP_CONFIGURE 'remote admin connections', 0
RECONFIGURE
```

VKEY: V0015651	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: EBRP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.4.2			
STIG Requirement:	(DG0157: CAT II) The DBA will ensure remote administration of the database is not enabled or configured unless mission and/or operationally required and authorized by the IAO.			

4.96 DG0158: DBMS remote administration audit

Description: When remote administration is available, the vulnerability to attack for administrative access is increased. An audit of remote administrative access provides additional means to discover suspicious activity and to provide accountability for administrative actions completed by remote users.

Check:

If the DBMS does not provide auditing of remote administrative actions, this check is Not a Finding.

Review settings for actions taken during remote administration sessions.

If auditing of remote administration sessions and actions is not enabled, this is a Finding.

If audit logs do not include all actions taken by database administrators during remote sessions, this is a Finding.

Actions should be tied to a specific user.

Fix:

Develop, document and implement policy and procedures for remote administration auditing.

Configure the DBMS to provide an audit trail for remote administrative sessions. Include all actions taken by database administrators during remote sessions.

Actions should be tied to a specific user.

VKEY: V0015652	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: EBRP	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.4.2			
STIG Requirement:	(DG0158: CAT II) The DBA will configure auditing of all actions taken by database administrators during remote sessions.			

4.97 DG0159: Review of DBMS remote administrative access

Description: Remote administrative access to systems provides a path for access to and exploit of DBA privileges. Where the risk has been accepted to allow remote administrative access, it is imperative to instate increased monitoring of this access to detect any abuse or compromise.

Check:

If remote administrative access to the database is disabled, this check is Not a Finding.

Review policy, procedures and implementation evidence of monitoring of remote administrative access to the database with the IAO or IAM.

If policy and procedures for monitoring remote administrative access do not exist or not implemented, this is a Finding.

Fix:

Develop, document and implement policy and procedures to monitor remote DBA access to the DBMS.

The automated generation of a log report with automatic dissemination to the IAO and/or IAM may be used. Require and store an acknowledgement of receipt and confirmation of review for the log report.

VKEY: V0015118	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: EBRP	Check Type: Interview	Database Level: False	Responsibility: IAO / IAM	Documentable: False
Reference:	Database STIG 3.4.2			
STIG Requirement:	(DG0159: CAT II) The IAO or IAM will review daily audit trails of remote administrative sessions to discover any unauthorized access or actions.			

4.98 DG0161: DBMS audit tool

Description: Audit logs can capture information on suspicious events. Without an automated monitoring and alerting tool, malicious activity may go undetected and without response until compromise of the database or data is severe.

Check:

Review evidence or operation of audit tool monitoring and alerts with the IAO.

If a monitoring tool that provides alerts is not implemented, this is a Finding.

Fix:

Develop or procure, document and implement an automated tool that monitors audit logs and generates automated alerts.

Compliance may be accomplished using existing database features.

VKEY: V0015103	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-C
IA Control: ECAT	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.3			
STIG Requirement:	(DG0161: CAT II) The IAO will ensure an automated monitoring tool or capability is employed to review DBMS audit data and immediately report suspicious or unauthorized activity.			

4.99 DG0167: Encryption of DBMS sensitive data in transit

Description: Sensitive data served by the DBMS and transmitted across the network in clear text is vulnerable to unauthorized capture and review.

Check:

If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan and/or AIS Functional Architecture documentation, this check is Not a Finding.

If encryption requirements are listed and specify configuration at the host system or network device level, review evidence that the configuration meets the specification with the DBA. It may be necessary to review network device configuration evidence or host communications configuration evidence with a Network and/or System Administrator.

If the evidence review does not meet the requirement or specification as listed in the System Security Plan, this is a Finding.

For SQL Server 2005:

If encryption for sensitive data in transit is required by SQL Server configuration, then review the setting for the instance parameter ForceEncryption:

From the SQL Server Configuration Manager GUI:

1. Expand SQL Server 2005 Network Configuration
2. Right-click on Protocols for [instance name]
3. Select Properties
4. Select the Flags tab
5. View the value for ForceEncryption

OR

From the Registry Editor:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.1 \ MSSQLServer \ SuperSocketNetLib \ ForceEncryption

If the value of ForceEncryption does not equal yes or 1, this is a Finding

Fix:

Configure encryption of sensitive data served by the DBMS in accordance with the specifications provided in the System Security Plan.

Document acceptance of risk by the Information Owner where sensitive or classified data is not encrypted. Have the IAO document assurance that the unencrypted sensitive or classified information is otherwise inaccessible to those who do not have Need-to-Know access to the data.

For SQL Server 2005:

Also, see Microsoft KB article for information on using SQL Server in FIPS 140-2 compliant mode:

http://support.microsoft.com/kb/920995/

To configure encryption using SQL Server features:

From the SQL Server Configuration Manager GUI:

1. Expand SQL Server 2005 Network Configuration
2. Right-click on Protocols for [instance name]
3. Select Properties
4. Select the Flags tab
5. Select Yes for ForceEncryption from the pull-down options

VKEY: V0015104	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECCT	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.6			
STIG Requirement:	(DG0167: CAT I) The DBA will ensure database communications are encrypted when transmitting sensitive data across untrusted network segments and in accordance with the application requirements.			

4.100 DG0175: DBMS host and component STIG compliancy

Description: The security of the data stored in the DBMS is also vulnerable to attacks against the host platform, calling applications, and other application or optional components.

Check:

Review evidence of security hardening and auditing of the DBMS host platform with the IAO. If the DBMS host platform has not been hardened and received a security audit, this is a Finding.

Review evidence of security hardening and auditing for all application(s) that store data in the database and all other separately configured components that access the database including web servers, application servers, report servers, etc. If any have not been hardened and received a security audit, this is a Finding.

Review evidence of security hardening and auditing for all application(s) installed on the local DBMS host where security hardening and auditing guidance exists. If any have not been hardened and received a security audit, this is a Finding.

Fix:

Configure all related application components and the DBMS host platform in accordance with the applicable DOD STIG. Regularly audit the security configuration of related applications and the host platform to confirm continued compliance with security requirements.

VKEY: V0015116	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECSC	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.19			
STIG Requirement:	(DG0175: CAT II) The IAO will ensure the DBMS host and related applications and components comply with all applicable DOD STIGs.			

4.101 DG0176: DBMS audit log backups

Description: DBMS audit logs are essential to the investigation and prosecution of unauthorized access to the DBMS data. Unless audit logs are available for review, the extent of data compromise may not be determined and the vulnerability exploited may not be discovered. Undiscovered vulnerabilities could lead to additional or prolonged compromise of the data.

Check:

Audit events are logged by SQL Server to error logs, Windows event logs, and to SQL Profiler trace files.

Review evidence of backups that include the default directory for SQL Server error logs and trace files.

SQL Server 7 & 2000:

The default directory specification is stored in the Windows registry under:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLSERVER \ MSSQLServer \ DefaultLog

SQL Server error log files:

ERRORLOG.[#]

Audit trace (*.trc) files:

A default directory is not specified. Trace files may be directed to any accessible directory.

SQL Server Agent Log File:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLSERVER \ MSSQLServer \ SQLServerAgent \ ErrorLogFile

SQL Server 2005:

The default directory for SQL Server error logs and trace files is stored in the Windows registry under:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ MSSQLServer \ DefaultLog

Where [#] is the sequential number assigned to each instance.

This directory is referred to below as [instance logpath]:

SQL Server error logs:

[instance logpath]ERRORLOG.[#]

Audit trace (*.trc) files:

Default is [instance logpath], but may be directed to any accessible directory.

Log files of other components, e.g. SQLAGENT.[#]:

[instance logpath]

Audit trace results may also be directed to SQL Server tables. SQL Server data backups are addressed in a separate check; therefore, do not include audit results stored in database tables.

If evidence of inclusion of audit log files in regular DBMS or host backups does not exist, this is a Finding.

Fix:

Configure and ensure SQL Server audit trace files, instance and other error log files are included in regular backups.

VKEY: V0015117	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-C
IA Control: ECTB	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.21			
STIG Requirement:	(DG0176: CAT II) The DBA will ensure the DBMS audit logs are included in DBMS backup procedures.			

4.102 DG0186: DBMS network perimeter protection

Description: Databases often store critical and/or sensitive information used by the organization. For this reason, databases are targeted for attacks by malicious users. Additional protections provided by network defenses that limit accessibility help protect the database and its data from unnecessary exposure and risk.

Check:

Review the System Security Plan and AIS Functional Architecture documentation to determine if the database serves data to users or applications outside the local enclave.

If the database is not accessed outside of the local enclave, this is Not a Finding.

If the database serves applications available from a public network (e.g. the Internet), then confirm that it is located in a DMZ.

If the database is directly accessible to public users, this is a Finding.

If the database serves public-facing applications and not protected by location in a DMZ, this is a Finding.

Fix:

Do not allow direct connections from users originating from the Internet or other public network to the database.

Locate the database in a DMZ if it serves data to public-facing applications. Do not locate a database that serves public-facing applications inside the local intranet.

Include in the System Security Plan and AIS Functional Architecture documentation for the system whether the database serves public-facing applications or applications serving users from other untrusted networks.

VKEY: V0015122	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-SP;2-SP;3-SP
IA Control: EBBD	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.4.1			
STIG Requirement:	(DG0186: CAT II) The IAO will ensure the DBMS is protected from direct client connections from public or unauthorized networks.			

4.103 DG0187: DBMS software file backups

Description: The DBMS application depends upon the availability and integrity of its software libraries. Without backups, compromise or loss of the software libraries can prevent a successful recovery of DBMS operations.

Check:

Review evidence of SQL Server and dependent application files and directories.

SQL Server 7 & 2000:

The SQL Server software directory is specified in the registry value:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ Setup \ SQLPath

Other SQL Server software including, but not limited to SQL Server tools and utilities, are found in the directory and subdirectories under:

[drive] \ Program Files \ Microsoft SQL Server

This directory is specified in the registry under:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ [70 or 80] \ Tools \ ClientSetup \ SQLPath

SQL Server 2005:

The SQL Server software directory is specified in the registry value:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ Setup \ SqlBinRoot

Other SQL Server software including, but not limited to SQL Server tools and utilities, are found in the directory and subdirectories under:

[drive] \ Program Files \ Microsoft SQL Server

This directory is specified in the registry under:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ 90 \ Tools \ Setup \ SQLPath

Other executables may be installed under the same Microsoft SQL Server path.

Third-party applications may be located in other directory structures.

Review the System Security Plan for a list of all DBMS application software libraries to be included in software library backups.

If any software library files are not included in regular backups, this is a Finding.

Fix:

Configure backups to include all DBMS application and third-party database application software libraries.

VKEY: V0015121	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: COSW	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.5.4			
STIG Requirement:	(DG0187: CAT II) The DBA will ensure critical database software directories are backed up.			

4.104 DG0190: DBMS remote system credential use and access

Description: Credentials defined for access to remote databases or applications may provide unauthorized access to additional databases and applications to unauthorized or malicious users.

Check:

Review the list of defined database links generated from the DBMS:

For SQL Server 7 & 2000:

```
SELECT srvname
FROM [master].dbo.sysservers
WHERE srvid <> 0
ORDER BY srvname
```

For SQL Server 2005:

```
SELECT name
FROM [master].sys.servers
WHERE server_id <> 0
ORDER BY name
```

Compare to the list in the System Security Plan with the DBA.

If no linked servers are listed in the database and in the System Security Plan, this check is Not a Finding.

If any linked servers are listed, verify the authorization for the definition in the System Security Plan.

If any linked servers exist that are not authorized or not listed in the System Security Plan, this is a Finding.

For all authorized servers, review user access to the links:

For SQL Server 7 & 2000:

```
SELECT name
FROM [master].dbo.syslogins
WHERE sid <> 0x01
ORDER BY name
```

For each name listed, confirm in the System Security Plan that they are authorized for access to the linked server.

For SQL Server 2005:

```
SELECT server_id, USER_NAME(local_principal_id) 'User'
FROM [master].sys.linked_logins
WHERE server_id <> 0
ORDER BY server_id
```

A NULL user name indicates a grant to PUBLIC or a wildcard username.

For each local_principal_id listed, confirm in the System Security Plan that they are authorized for access to the linked server.

For any linked server login mapping that specifies a NULL local_principal_id, this is a Finding.

If access to any linked server has been granted to an unauthorized user, this is a Finding.

Fix:

Grant access to linked servers to authorized users or applications only.

Document all linked server access authorizations in the System Security Plan.

VKEY: V0015154	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0190: CAT II) The DBA will ensure credentials used to access remote databases or other applications are restricted to authorized database accounts and used only for mission and/or operationally required and documented purposes.			

4.105 DG0194: DBMS developer privilege monitoring on shared DBMS

Description: The developer role does not require Need-to-Know or administrative privileges to production databases. Assigning excess privileges can lead to unauthorized access to sensitive data or compromise of database operations.

Check:

If the DBMS or DBMS host is not shared by production and development activities, this check is Not a Finding.

Review policy, monitoring procedures and evidence of developer privileges on shared development and production DBMS and DBMS host systems with the IAO.

If developer privileges are not monitored every three months or more frequently, this is a Finding.

Fix:

Develop, document and implement policy and procedures to monitor DBMS and DBMS host privileges assigned to developers on shared production and development systems to detect unauthorized assignments every three months or more often.

VKEY: V0015108	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECPC	Check Type: Interview	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.15			
STIG Requirement:	(DG0194: CAT II) The IAO will review privileges granted to developers on shared production/development database systems that allow modification of application code or application objects every three months or more frequently.			

4.106 DG0195: DBMS host file privileges assigned to developers

Description: Developer roles should not be assigned DBMS administrative privileges to production DBMS application and data directories. The separation of production and development DBA and developer roles help protect the production system from unauthorized, malicious or unintentional interruption due to development activities.

Check:

If the DBMS host does not support both production and development operations, this check is Not a Finding.

Review the list of OS DBA group membership with the SA and DBA. Compare to the list in the System Security Plan.

If any accounts not identified in the System Security Plan for the production DBMS have been assigned DBA privileges (to include developer accounts), this is a Finding.

If OS DBA group membership is not included in the System Security Plan, this is a Finding.

Fix:

Create separate DBMS host OS groups for developer and production DBAs.

Do not assign production DBA accounts to development OS groups. Do not assign development DBA accounts to production OS groups.

Remove any unauthorized accounts from both production and development OS groups.

Document in the System Security Plan

VKEY: V0015109	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECPC	Check Type: Interview	Database Level: False	Responsibility: SA/DBA	Documentable: False
Reference:	Database STIG 3.3.15			
STIG Requirement:	(DG0195: CAT II) The SA/DBA will ensure developer accounts on a shared production/development host system are not granted operating system privileges to production files, directories or database components.			

4.107 DG0198: DBMS remote administration encryption

Description: Remote administration provides many conveniences that can assist in the maintenance of the designed security posture of the DBMS. On the other hand, remote administration of the database also provides malicious users the ability to access from the network a highly privileged function. Remote administration needs to be carefully considered and used only when sufficient protections against its abuse can be applied. Encryption and dedication of ports to access remote administration functions can help prevent unauthorized access to it.

Check:

If remote administration is disabled or not configured, this check is Not a Finding.

Review configured network access interfaces for remote DBMS administration with the SA and DBA. These may be host-based encryptions such as IPSec or may be configured for the DBMS as part of the network communications and/or in the DBMS listening process. For DBMS listeners, verify that encrypted ports exist and are restricted to specific network addresses to access the DBMS. View the System Security Plan to review the authorized procedures and access for remote administration.

If the configuration does not match the documented plan, this is a Finding.

Fix:

Disable remote administration where it is not required or authorized. Consider restricting administrative access to local connections only. Where necessary, configure the DBMS network communications to provide an encrypted, dedicated port for remote administration access.

Develop and provide procedures for remote administrative access to DBAs that have been authorized for remote administration. Verify during audit reviews that DBAs do not access the database remotely except through the dedicated and encrypted port.

VKEY: V0015662	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: EBRP	Check Type: Interview	Database Level: False	Responsibility: SA/DBA	Documentable: False
Reference:	Database STIG 3.4.2			
STIG Requirement:	(DG0198: CAT II) The SA/DBA will ensure remote administration connections to the database are restricted to dedicated and encrypted network addresses and ports.			

4.108 DM0510: C2 audit mode

Description: The C2 audit mode uses a system-defined trace to collect audit information for MS SQL Server 2000 and higher. It utilizes all security event categories defined within SQL Server, not all of which are required by the Database STIG. Without required auditing, accountability and investigative support is limited.

Check:

For SQL Server 2000:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].dbo.sysconfigures
WHERE comment = 'c2 audit mode'
```

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'c2 audit mode'
```

If 1 is returned as the value for Config_Value, this is Not a Finding

If the value 0 is returned for Config_Value, confirm that a valid audit trace is configured and implemented. See checks DG0029, DG0145 and DM5267. If there is not a valid audit trace, this is a Finding.

Fix:

Configure and enable C2 auditing or confirm valid audit traces are set per checks DG0029, DG0145 and DM5267.

Note: Setting the C2 audit mode enables auditing of more events than required by the STIG and may generate too many records to manage effectively.

For SQL Server 2000 and 2005:

From the query prompt:

```
EXEC SP_CONFIGURE 'c2 audit mode', 1
RECONFIGURE
```

To create a custom audit, see instructions in check DG0145.

VKEY: V0002426	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAT	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.2			
STIG Requirement:	(DG0145: CAT II) The DBA will ensure audit records contain the user ID, date and time of the audited event, and the type of the event.			

4.109 DM0530: Fixed server role members

Description: Fixed server roles provide a mechanism to grant groups of privileges to users. These privilege groupings are defined by the installation or upgrade of the SQL Server software at the discretion of Microsoft. Memberships in these roles granted to users should be strictly controlled and monitored. Privileges assigned to these roles should be reviewed for change after software upgrade or maintenance to ensure that the privileges continue to be appropriate to the assigned members.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
EXEC SP_HELPSRVROLEMEMBER 'dbcreator'
EXEC SP_HELPSRVROLEMEMBER 'diskadmin'
EXEC SP_HELPSRVROLEMEMBER 'processadmin'
EXEC SP_HELPSRVROLEMEMBER 'securityadmin'
EXEC SP_HELPSRVROLEMEMBER 'setupadmin'
```

For SQL Server 2005:

From the query prompt:

```
EXEC SP_HELPSRVROLEMEMBER 'bulkadmin'
EXEC SP_HELPSRVROLEMEMBER 'dbcreator'
EXEC SP_HELPSRVROLEMEMBER 'diskadmin'
EXEC SP_HELPSRVROLEMEMBER 'processadmin'
EXEC SP_HELPSRVROLEMEMBER 'securityadmin'
EXEC SP_HELPSRVROLEMEMBER 'serveradmin'
EXEC SP_HELPSRVROLEMEMBER 'setupadmin'
EXEC SP_HELPSRVROLEMEMBER 'sysadmin'
```

Verify authorization of each member listed in the System Security Plan. If any members are not authorized, this is a Finding.

Fix:

Remove fixed server role assignments from unauthorized users. Grant fixed roles to authorized personnel only. Remove unauthorized accounts from assigned roles.

From the query prompt:

```
EXEC SP_DROPSRVROLEMEMBER '[account name]', '[fixed server role name]'
```

Replace [account name] with the name of the account and [fixed server role name] with the name of the fixed server role

VKEY: V0002427	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0119: CAT II) The DBA will ensure database application user roles are restricted to select, insert, update, delete, and execute privileges.			

4.110 DM0660: MS SQL Server instance name

Description: The use of version numbers within the database instance name restricts the use of the instance name from meaningful use in subsequent upgrades. Changing the database instance names on a production database causes unnecessary administrative overhead and compromise existing secure network configurations.

Check:

For SQL Server 2000 & 2005:

From the query prompt:

```
SELECT RTRIM(CONVERT(CHAR(20),
SERVERPROPERTY('instancename')))
```

If the instance name contains the SQL Server version number, this is a Finding.

Fix:

For SQL Server 2000 & 2005:

Do not use version number references or default names for instance names.

The instance name cannot be changed on an existing instance.

A new instance can be created with a compliant name and the databases moved.

VKEY: V0002436	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECAN	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0123: CAT II) The DBA will ensure all access to sensitive application data stored inside the database, and in external host files, is granted only to database accounts and OS accounts in accordance with user functions as specified by the Information Owner.			

4.111 DM0900: SQL and database mail use

Description: The SQL Mail, SQL Mail Extended Stored Procedures (XPs) and Database Mail XPs are used by database applications to provide email messages to and from the database. This capability may easily be abused to send malicious messages to remote users or systems. Disabling its use helps to protect the database from generating or receiving malicious email notifications.

Check:

Determine the SQL Server Edition:

From the query prompt:

```
SELECT CONVERT(INT, SERVERPROPERTY('EngineEdition'))
```

If value returned is 1 (Personal or Desktop Edition) or 4 (Express Edition), this check is Not Applicable.

For SQL Server 7 & 2000:

From the SQL Sever Enterprise Manager GUI:

1. Expand SQL server name
2. Expand Support Services
3. Right click on SQL Mail

If profile name is not blank, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'sql mail xps'
```

If the value of Config_Value is 0, this is Not a Finding.

If the value of Config_Value is 1, then confirm in the System Security Plan that email message traffic is required by the database applications. If it is not documented, and required this is a Finding.

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
```

WHERE name = 'database mail xps'

If the value of Config_Value is 0, this is Not a Finding.

If the value of Config_Value is 1, then confirm in the System Security Plan that email message traffic is required by the database applications. If it is not documented, and required this is a Finding.

Fix:

Ensure you properly document SQL Mail, SQL Mail XPs and Database Mail XPs configurations regardless of authorization or use in the System Security Plan.

If not approved by the IAO and authorized for use, disable SQL Mail, SQL Mail XPs and Database Mail XPs.

For SQL Server 7 & 2000:

From the SQL Server Enterprise Manager GUI:

1. Expand SQL server name
2. Expand Support Services
3. Right click on SQL Mail
4. Delete the name of the profile listed in the profile name text box

For SQL Server 2005:

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'SQL Mail XPs', 0
RECONFIGURE
```

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'Database Mail XPs', 1
RECONFIGURE
```

VKEY: V0003335	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.112 DM0901: SQL Server Agent email notification

Description: SQL Mail accepts incoming database commands via email. This can introduce malicious codes or viruses into the SQL server environment.

Check:

Determine the SQL Server Edition:

From the query prompt:

```
SELECT CONVERT(INT, SERVERPROPERTY('EngineEdition'))
```

If value returned is 1 (Personal or Desktop Edition) or 4 (Express Edition), this check is Not Applicable.

For SQL Server 7 & 2000:

From the SQL Server Enterprise Manager GUI:

1. Expand SQL server name
2. Expand Management
3. Right click on SQLServerAgent

If profile name is not blank, documentation for this function should exist with the IAO in the System Security Plan and AIS Functional Architecture documentation.

If this function is not documented, this is a Finding.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Right click on SQL Server Agent
2. Select Properties
3. Select Alert System

If the box next to "Enable mail profile" is checked, documentation for this function should exist with the IAO in the System Security Plan and AIS Functional Architecture documentation.

If this function is not documented, this is a Finding.

Fix:

Ensure you properly document Agent Email Alert configurations regardless of authorization or use in the System Security Plan.

Where not required and authorized for use, disable Email notification for SQL Server Agent.

VKEY: V0003336	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCBP	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.113 DM0919: SQL Server services Windows group membership

Description: Exploits to SQL Server services may provide access to the host system resources within the security context of the service. Excess privileges assigned to the SQL Services can increase the threat to the host system.

Check:

View the Windows group memberships assigned to the SQL Server service accounts:

SQL Server 7 & 2000:

List of services:

1. SQL Server Database
2. SQL Server Agent

SQL Server 2005:

List of services:

1. SQL Server Database
2. SQL Server Agent
3. Analysis Services
4. Integration Services
5. Reporting Services
6. Notification Services
7. Full Text Search
8. SQL Server Browser
9. SQL Server Active Directory Helper
10. SQL Writer

Group Membership:

The service account and groups should be local unless the services access other domain or remote services.

1. Service-specific groups (e.g. SQLServer2005MSSQLUser$[host name]$[instance name])
2. SQL Server services Users Groups - custom name, used to replace Users group permissions to SQL Server directories and files
3. Performance Monitor - for SQL Server Database service if Replication is in use and performance is monitored
4. Windows Users group

If any services are assigned group membership to any groups other than:

1. A custom SQL Server service group
2. A custom SQL Server service users group,
3. Windows Users group

this is a Finding.

User rights and file permissions are reviewed under separate checks.

Fix:

Remove unnecessary group membership from SQL Server service accounts. Review any group membership assignments other than the:

1. SQL Server service group
2. SQL Server service users group
3. Windows Users group

For SQL Server Database service, Performance Monitor group membership if replication and monitoring are operationally required.

VKEY: V0015170	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECPA	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.14			
STIG Requirement:	(DG0117: CAT II) The IAO will ensure all database administrative privileges defined within the DBMS and externally to the database are assigned using DBMS or OS roles.			

4.114 DM0920: Custom OS DBA group

Description: The DBA job function differs from the host system administrator job function. Without a separate host OS group to assign necessary privileges on the operating system, separation of duties is not achieved and excess privileges for the job function are assigned.

Check:

For Windows 2000:

1. Right click on My Computer
2. Select Manage
3. Expand Local Users
4. Expand Groups

For Windows 2003:

1. Click Start
2. Select All Programs
3. Select Administrative Tools
4. Click Computer Management
5. Expand System Tools
6. Expand Local Users and Groups
7. Select Groups

View the list of groups defined. Verify the OS DBA group as specified in the System Security Plan exists.

If the OS DBA windows group specified in the System Security Plan does not exist, this is a Finding.

Fix:

Follow the steps outlined in the Check procedure above. Create a Windows OS group to use for SQL Server DBA privilege and permission assignment as documented in the System Security Plan.

VKEY: V0003832	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECPA	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.14			
STIG Requirement:	(DG0117: CAT II) The IAO will ensure all database administrative privileges defined within the DBMS and externally to the database are assigned using DBMS or OS roles.			

4.115 DM0921: DBA OS privilege assignment

Description: The host DBA group is assigned permissions to the DBMS system libraries and may be used to assign DBA privileges within the database. Unauthorized DBA privilege assignment leaves the DBMS data and operations vulnerable to complete compromise.

Check:

For Windows 2000:

1. Right click on My Computer
2. Select Manage
3. Expand Local Users
4. Expand Groups
5. Select the OS DBA Group
6. Right click on the OS DBA Group
7. Select Properties

For Windows 2003:

1. Click Start
2. Select All Programs
3. Select Administrative Tools
4. Click Computer Management
5. Expand System Tools
6. Expand Local Users and Groups
7. Select Groups
8. Select the OS DBA Group
9. Right click on the OS DBA Group
10. Select Properties

Review the list of accounts assigned to the OS DBA group.

Review the list of accounts assigned to the SYSADMIN role:

For SQL Server:

From the query prompt:

```
EXEC SP_HELPSRVROLEMEMBER 'sysadmin'
```

If any accounts assigned OS DBA group membership or SYSADMIN privileges that are not DBAs as authorized and documented in the System Security Plan, this is a Finding.

If the OS DBA group is not defined, this is a Finding.

Fix:

Remove any OS DBA group membership assignments and assignments to the SYSADMIN role from accounts not authorized and documented in the System Security Plan by the IAO.

Authorize and document in the System Security Plan all DBA accounts and assignments to the SYSADMIN role prior to assigning DBA group membership and privileges.

VKEY: V0003833	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECPA	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.14			
STIG Requirement:	(DG0117: CAT II) The IAO will ensure all database administrative privileges defined within the DBMS and externally to the database are assigned using DBMS or OS roles.			

4.116 DM0924: SQL server service account

Description: The Windows builtin Administrators group and LocalSystem account are assigned full privileges to the Windows operating system. These privileges are not required by the SQL Server service accounts for operation and, if assigned, could allow a successful attack of the SQL Server service to lead to a full compromise of the host system.

Check:

Check for Service Account used:

For Windows 2003 (Windows 2000 is similar):

1. Click Start
2. Right click on My Computer
3. Click on Manage,
4. Expand Services and Applications
5. Select Services
6. Locate the MSSQLServer services (SQL Server 7 & 2000) or SQL Server ([instance name]) services (SQL Server 2005)
7. Examine the account listed in the 'Log On As' column

If the account listed is a builtin account (LocalSystem, Local Service, Network Service, etc.), this is a Finding.

Exceptions with SQL Server 2005 are:

1. SQL Server Active Directory Helper (Network Service)
2. SQL Server Integration Services (Network Service)
3. SQL Server VSS Writer (Local System)

If the account listed is a domain user account (does not begin with ".\" or the host computer name), then confirm that the service requires access to remote systems including for the provision of email services as documented in the System Security Plan.

If network resource access is not required, use of domain account is a Finding.

If the account listed is a local or domain user account, then review group membership privileges. See below for Administrator group privilege check. Note any other group membership assignments for future check analysis.

For Windows 2000:

1. Right click on My Computer
2. Select Manage
3. Expand Local Users

4. Expand Groups
5. Select the Administrators Group
6. Right click on the Administrators Group
7. Select Properties

For Windows 2003:

1. Click Start
2. Select All Programs
3. Select Administrative Tools
4. Click Computer Management
5. Expand System Tools
6. Expand Local Users and Groups
7. Select Groups
8. Select the Administrators Group
9. Right click on the Administrators Group
10. Select Properties

If the service account is listed as a member of the Administrators group, this is a Finding.

Note: SQL Server Agent cannot be configured for autorestart without assignment to the Administrator Group. SQL Server Agent must be manually restarted after the service has been interrupted.

Fix:

Create a local custom account for the SQL Server service accounts. A domain account may be used where network resources are required.

Please see SQL Server Books Online for information that is more detailed.

Assign the service accounts to the SQL Server groups created at installation (SQL Server 2005) if available.

Assign the SQL Server accounts to the appropriate OS SQL Service group. Do not assign the SQL Server accounts to the OS DBA group.

Note: Each service identified with an ([Instance Name]) should have its own, separate local user/domain user account. Do not add the SQL Server Agent user/domain account to the local or domain Administrators groups.

VKEY: V0003835	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: SA / DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0101: CAT II) The DBA will ensure OS accounts used for execution of external database procedures have the minimum OS privileges required assigned to them.			

4.117 DM0927: SQL server registry keys permissions

Description: Registry keys contain configuration data for the SQL Server services and applications. Unrestricted access or access unnecessary for operation can lead to a compromise of the application or disclosure of information that may lead to a successful attack or compromise of data.

Check:

Use regedit.exe (Windows 2003) or regedt32.exe (Windows XP, Windows 2000) to review registry permissions

To review registry permissions using regedit.exe, navigate to the registry key indicated, right-click on the key, and select Permissions. Select the users and groups permissions and view the assigned Permissions in the Permissions box.

To view Special Permissions (From the Permissions window for the key):

1. Click on the Advanced button
2. Select the Effective Permissions tab
3. Click the Select button
4. Select the User or Group name to review
5. To see the list of users or groups:
    a. Click on the Advanced button
    b. Click on the Find Now button
    c. Select a user or group account
    d. Click OK

Note: QENR (used below) indicates Special Permissions Query Value (Q), Enumerate Subkeys (E), Notify (N), Read Control (R)

View registry permissions for the following registry keys and sub-keys under:

For SQL Server 7 & 2000:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer

For SQL Server 2005:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server

If Full Control permissions are granted to other than Administrators, the DBA group, Creator Owner, System or the SQL Server service group with the following exceptions, this is a Finding.

1. HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ Instance Names \ RS \ = Full Control to key to local group account SQLServer2005ReportServerUser$[instance name]
2. HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.1 \ MSSearch \ = Full Control to keys and Subkeys to local group account SQLServer2005MSFTEUser$[instance name]
3. HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.1 \ SQLServerAgent \ = Full Control to key to local group account SQLServer2005SQLAgentUser$[instance name]
4. HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.1 \ SQLServerAgent \ = Full Control to key to local group account SQLServer2005SQLServerADHelperUser$[instance name]
5. HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ Instance Names \ RS \ = Read to keys and Subkeys to local group account Remote Desktop Users

If other than Read permissions are granted to the custom SQL Server Users group or members of that group, this is a Finding.

Note: During SQL Server 2005 installation, service group memberships are granted Read access to specific registry keys. If this Read access duplicates the custom SQL Server Users group access, this would not be a Finding.

The DBA, Creator Owner, System, Administrators and SQL Server service groups should be granted Full Control.

Fix:

Review permissions assigned to the SQL Server registry keys and Subkeys.

Revoke Full Control permissions to accounts or groups other than DBAs, Administrators, System and Creator Owner except for keys and Subkeys listed in the check procedures.

Revoke all Read permissions from any custom SQL Server users group and specific other groups as listed in the check procedures.

VKEY: V0003838	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECAN	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0123: CAT II) The DBA will ensure all access to sensitive application data stored inside the database, and in external host files, is granted only to database accounts and OS accounts in accordance with user functions as specified by the Information Owner.			

4.118 DM0928: SQL Server component service account user rights

Description: Excessive or unneeded privileges allow for unauthorized actions. When application vulnerabilities are exploited, excessive privileges assigned to the application can lead to unnecessary risk to the host system and other services.

Check:

Check User Rights (may be assigned using group privileges):

1. Click Start
2. Select Control Panel \ Administrative Tools (Win2K) or Select Administrative Tools (Win2K3)
3. Click Local Security Policy
4. Expand Local Policies
5. Select User Rights Assignment

View the Security Settings to see user rights assigned to the service account or group.

If any user rights are assigned to the service account other than the following, this is a Finding.

If any services listed below do not exist, then do not include them in the review:

1. Analysis Server: Log on as a service
2. Report Server: Log on as a service
3. Integration Services:
    a. Log on as a service
    b. Permission to write to application event log
    c. Bypass traverse checking
    d. Create global objects
    e. Impersonate a client after authentication
4. Full-Text Search: Log on as a Service
5. SQL Server Browser: Log on as a Service

Fix:

Create local custom accounts for the SQL Server Analysis, Reporting, Full Text Search, and Browser service accounts. A domain account may be used where network resources are required. Please see SQL Server Books Online for information that is more detailed.

Assign the service account to the SQL Server service group (created at installation for the service accounts for SQL Server 2005) if available.

Assign the service account or group the user privileges as listed in the Check procedures.

VKEY: V0015169	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: SA / DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0101: CAT II) The DBA will ensure OS accounts used for execution of external database procedures have the minimum OS privileges required assigned to them.			

4.119 DM0929: Integration services OS account least privilege

Description: Excess privileges can unnecessarily increase the vulnerabilities to a successful attack. If the Integration Service is compromised, the attack can lead to use of the privileges assigned to the service account. Administrative and other unnecessary privileges assigned to the service account can be used for an attack on the host system and/or SQL Server database.

Check:

For SQL Server 2005:

Check User Rights (may be assigned using group privileges):

1. Click Start
2. Select Control Panel \ Administrative Tools (Win2K) or Select Administrative Tools (Win2K3)
3. Click Local Security Policy
4. Expand Local Policies
5. Select User Rights Assignment

The SQL Server services and associated service accounts (under the Logon As column) can be viewed using the Windows Services Snap-In.

View the Security Settings to see user rights assigned to the service account or group.

For SQL Server Integration Services service account:

If any user rights are assigned to the service account other than the following, this is a Finding:

1. Log on as a service (SeServiceLogonRight)
2. Permission to write to application event log
3. Bypass traverse checking (SeChangeNotifyPrivilege)
4. Create global objects (SeCreateGlobalPrivilege)
5. Impersonate a client after authentication (SeImpersonatePrivilege)

Fix:

For SQL Server 2005:

Create a local custom account for the Integration Services service account. A domain account may be used where network resources are required. Please see SQL Server Books Online for information that is more detailed.

Assign the account to the Integration Services group (created at installation for SQL Server 2005) if available.

Assign the Integration Services account or group the user privileges as listed in the Check procedures.

VKEY: V0015134	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: SA / DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0101: CAT II) The DBA will ensure OS accounts used for execution of external database procedures have the minimum OS privileges required assigned to them.			

4.120 DM0933: SQL Server Agent account user rights

Description: Excess privileges can unnecessarily increase the vulnerabilities to a successful attack. If the SQL Server Agent service is compromised, the attack can lead to use of the privileges assigned to the service account. Administrative and other unnecessary privileges assigned to the service account can be used for an attack on the host system and/or SQL Server database.

Check:

Check User Rights (may be assigned using group privileges):

1. Click Start
2. Select Control Panel \ Administrative Tools (Win2K) or Select Administrative Tools (Win2K3)
3. Click Local Security Policy
4. Expand Local Policies
5. Select User Rights Assignment

View the Security Settings to see user rights assigned to the service account or group.

For SQL Server Agent service account:

If any user rights are assigned to the service account other than the following, this is a Finding:

1. Log on as a service (SeServiceLogonRight)
2. Act as part of the operating system (SeTcbPrivilege) (Win2K only)
3. Log on as a batch job (SeBatchLogonRight)
4. Replace a process-level token (SeAssignPrimaryTokenPrivilege)
5. Bypass traverse checking (SeChangeNotifyPrivilege)
6. Adjust memory quotas for a process (SeIncreaseQuotaPrivilege)

Fix:

Create a local custom account for the SQL Server Agent service account. A domain account may be used where network resources are required. Please see SQL Server Books Online for information that is more detailed.

Assign the account to the SQL Server Agent (group created at installation for SQL Server 2005) if available.

Assign the SQL Server Agent account or group the user privileges as listed in the Check procedures.

VKEY: V0015155	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: SA / DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0101: CAT II) The DBA will ensure OS accounts used for execution of external database procedures have the minimum OS privileges required assigned to them.			

4.121 DM1757: Direct access to system table updates

Description: The allow updates option determines whether updates, deletes, or inserts can be executed on system tables. Stored procedures created when this option is turned on will have the ability to update system tables even after the option is turned off. Direct access and updates to the system tables bypasses integrity and security controls.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].dbo.sysconfigures
WHERE comment = 'allow updates to system tables'
```

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'allow updates'
```

If a value of 0 is returned for Config_Value, this is Not a Finding.

If a value of 1 is returned for Config_Value, confirm in the System Security Plan that this option is documented, required and approved by the IAO. If it is not documented, required and approved, this is a Finding.

Note: Some permission assigned to PUBLIC within the master database may require that the 'Allow modifications to be made directly to the system catalogs' database setting be temporarily enabled.

Fix:

Authorize and document requirements for use of the 'Allow updates to system tables' or 'allow updates' configuration option in the System Security Plan and AIS Functional Architecture documentation. Where not authorized, disable its use.

From the query prompt:

```
USE master
EXEC SP_CONFIGURE 'allow updates', 0
RECONFIGURE
```

VKEY: V0002460	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0122: CAT II) The DBA will ensure all access to sensitive administrative DBMS data stored inside the database and in external host files is granted only to DBA and other authorized administrative database and OS accounts.			

4.122 DM1758: xp_cmdshell option

Description: The xp_cmdshell extended stored procedures allows execution of host executables outside the controls of database access permissions. This access may be exploited by malicious users who have compromised the integrity of the SQL Server database process to control the host operating system to perpetrate additional malicious activity.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT u.name
FROM [master].dbo.sysobjects o, [master].dbo.sysusers u,
[master].dbo.sysprotects p
WHERE p.uid = u.uid
AND p.id = o.id
AND o.name = 'xp_cmdshell'
ORDER BY u.name
```

If any accounts are returned, ensure the IAO has documented in the System Security Plan allowing its use. If there is no documentation or use is not authorized, this is a Finding.

If any non-DBA accounts are listed, this is a Finding.

For SQL Server 2005:

Perform the check for SQL Server 7 & 2000 above in addition to the check listed below.

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'xp_cmdshell'
```

If a value of 0 is returned for Config_Value, this is Not a Finding.

If a value of 1 is returned for Config_Value, confirm in the System Security Plan that this option is documented, required and approved by the IAO. If it is not documented, required and approved, this is a Finding.

Fix:

Authorize and document requirements for use of the xp_cmdshell option in the System Security Plan and AIS Functional Architecture documentation. Where not authorized, disable or restrict its use.

For SQL Server 7 & 2000:

From the query prompt:

```
USE master
REVOKE EXECUTE ON xp_cmdshell FROM [user]
```

Replace 'user' with the user account name

For SQL Server 2005:

Perform the fix for SQL Server 7 & 2000 above if required and the fix below.

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'xp_cmdshell', 0
RECONFIGURE
```

VKEY: V0002461	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.123 DM1761: Scan for startup stored procedures option

Description: The DBMS startup process may be vulnerable to introduction of malicious or unauthorized actions. Any use of automated execution of custom procedures provides an opportunity to deploy unauthorized code. For some versions of SQL Server, audit requirements may only be met by audit procedures that are set to start automatically at system startup.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].dbo.sysconfigures
WHERE comment = 'scan for startup stored procedures'
```

If a value of 1 is returned for Config_Value and the SQL Server version is version 7, this is a Finding.

If a value of 0 is returned for Config_Value, the SQL Server version is version 8 and a custom audit trace is in use (see Check DG0145: DBMS audit record content), this is a Finding.

If a value of 1 is returned for Config_Value, the SQL Server version is version 8 and C2 Auditing is enabled (See Check DM0510**:** C2 audit mode), this is a Finding.

For SQL Server 2005:

Common Criteria (C2) mode requires a default audit trace to run at system startup. Therefore, this setting must always be set to 1 (TRUE). The existence of the default audit trace is verified in a separate check.

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'scan for startup procs'
```

If a value of 0 is returned for Config_Value, this is a Finding.

Fix:

For SQL Server 7 & 2000:

Disable the ‘scan for startup stored procedures’ configuration options if C2 audit mode is enabled unless a custom audit trace is defined:

From the query prompt:

```
EXEC SP_CONFIGURE 'scan for startup procedures', 0
```

For SQL Server 2005:

Enable the ‘scan for startup procs’ configuration option:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'scan for startup procs', 1
RECONFIGURE
```

Confirm that C2 Audit Mode is enabled or a custom audit trace is in use (see check DG0145).

VKEY: V0002464	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSS	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.12			
STIG Requirement:	(DG0155: CAT II) The DBA will ensure all applicable DBMS settings are configured to use trusted files, functions, features, or other components during startup, shutdown, aborts, or other unplanned interruptions.			

4.124 DM2095: OLE automation procedures option

Description: Extended stored procedures allow SQL Server users to execute functions external to SQL Server. An extended stored procedure is a function within a Windows DLL that can be referenced as a stored procedure. While this feature is a powerful extension of SQL Server, it also increases the risk of SQL Server users gaining unauthorized access to the operating system. The Windows account used by SQL Server to log on determines the security context used by extended stored procedures. Certain sensitive extended stored procedures should be closely monitored. These sensitive stored procedures include the OLE Automation stored procedures. OLE Automation stored procedures can be used to reconfigure the security of other services including IIS (Internet Information Server).

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT o.name 'Object', u.name 'User'
FROM [master].dbo.sysprotects p, [master].dbo.sysobjects o,
[master].dbo.sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND o.name like 'sp_OA%'
AND p.action = 224
AND p.protecttype IN (204, 205)
ORDER BY o.name, u.name
```

If no results are displayed, this is Not a Finding. If non-DBA users are granted access (as listed in the query results), verify with the IAO and the System Security Plan allowing the specific users listed as valid users of these procedures. If there is no documentation or IAO authorization, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'ole automation procedures'
```

If a value of 0 is returned for Config_Value, this is Not a Finding.

If a value of 0 is returned for Config_Value, verify with the IAO and the System Security Plan that OLE Automation Procedures as listed are required. If they are not, this is a Finding.

If OLE Automation Procedures are documented and authorized by the IAO, check which users have access.

From the query prompt:

```
SELECT o.name, USER_NAME(p.grantee_principal_id)
FROM [master].sys.system_objects o, [master].sys.database_permissions p
WHERE o.object_id = p.major_id
AND o.name like 'sp_OA%'
```

If non-DBA users are granted access, verify with the IAO and the System Security Plan allowing the specific users listed as valid users of these procedures. If there is no documentation or IAO authorization, this is a Finding.

Fix:

Delete OLE extended stored procedures from the database where not needed or restrict their access to SYSADMINs and authorized roles.

For SQL Server 7 & 2000:

From the query prompt (to drop):

```
USE master
EXEC SP_DROPEXTENDEDPROC ‘sp_OACreate’
EXEC SP_DROPEXTENDEDPROC ‘sp_OADestroy’
EXEC SP_DROPEXTENDEDPROC ‘sp_OAGetErrorInfo’
EXEC SP_DROPEXTENDEDPROC ‘sp_OAGetProperty’
EXEC SP_DROPEXTENDEDPROC ‘sp_OAMethod’
EXEC SP_DROPEXTENDEDPROC ‘sp_OAStop’
EXEC SP_DROPEXTENDEDPROC ‘sp_OASetProperty’
```

From the query prompt (to restrict):

```
USE master
REVOKE [permission] ON [object] FROM [user name]
```

For SQL Server 2005:

Disable OLE extended stored procedures:

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'OLE Automation Procedures', 0
RECONFIGURE
```

Note: SQL Server 2005 does not drop system extended stored procedures. Microsoft recommends denying EXEC permissions instead.

VKEY: V0002472	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.125 DM2119: Registry extended stored procedures access

Description: Extended stored procedures allow SQL Server users to execute functions external to SQL Server. An extended stored procedure is a function within a Windows NT DLL that can be referenced as a stored procedure. While this feature is a powerful extension of SQL Server, it also increases the risk of SQL Server users gaining unauthorized access to the operating system. The Windows NT account used by SQL Server to log on determines the security context used by extended stored procedures. Certain sensitive extended stored procedures should be closely monitored. These sensitive stored procedures include the registry editing stored procedures. Registry extended stored procedures can be used to read or change security information, including the NT password database, from the registry.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT o.name 'Object', u.name 'User'
FROM [master].dbo.sysprotects p, [master].dbo.sysobjects o,
[master].dbo.sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND o.name LIKE 'xp_reg%'
AND p.action = 224
AND p.protecttype IN (204, 205)
ORDER BY o.name, u.name
```

If no results are displayed, this is Not a Finding. If non-DBA users are granted access (as listed in the query results), verify with the IAO and the System Security Plan allowing the specific users listed as valid users of these procedures.

If there is no documentation or IAO authorization, this is a Finding.

If permissions are assigned to PUBLIC, this is a Finding.

Note: By default, the public role is granted execute access to xp_regread. If this access is required, transfer the privilege assignment to an authorized custom database role.

For SQL Server 2005:

From the query prompt:

```
SELECT o.name 'Object', u.name 'User'
```

```
FROM [master].sys.system_objects o, [master].sys.database_permissions p,
[master].sys.database_principals u
WHERE o.object_id = p.major_id
AND p.grantee_principal_id = u.principal_id
AND o.name LIKE 'xp_reg%'
AND p.type = 'EX'
ORDER BY o.name, u.name
```

If no results are displayed, this is Not a Finding. If non-DBA users are granted access (as listed in the query results), verify with the IAO and the System Security Plan allowing the specific users listed as valid users of these procedures. If there is no documentation or IAO authorization, this is a Finding.

If permissions are assigned to PUBLIC, this is a Finding.

Note: By default, the public role is granted execute access to xp_regread. If this access is required, transfer the privilege assignment to an authorized custom database role.

Fix:

For SQL Server 7 & 2000, delete registry extended stored procedures from the database where not needed.

For all versions of SQL Server, restrict access of Registry extended stored procedures to SYSADMINs and authorized roles.

Document restrictions in the System Security Plan

For SQL Server 7 & 2000:

From the query prompt (to drop):

```
USE master
EXEC SP_DROPEXTENDEDPROC '[procedure name]'
```

From the query prompt (to restrict):

```
USE master
REVOKE [permission] ON [object] FROM [user name]
```

For SQL Server 2005:

Note: SQL Server 2005 and later does not drop system extended stored procedures. Microsoft recommends denying EXEC permissions instead.

Restrict and/or remove access to Registry extended stored procedures:

From the SQL Server Management Studio GUI:

1. Connect/expand SQL Server
2. Expand Databases
3. Expand System databases
4. Expand Master
5. Expand Programmability
6. Expand Extended Stored Procedures
7. Expand System Extended Stored Procedures
8. Locate and select each of the Registry extended stored procedures listed in the Check section
9. Right click on the extended stored procedure
10. Select Properties
11. Click on the Permissions page
12. Select each user or role and deselect the Grant (and With Grant if checked) permissions from all users, database roles and public except from SYSADMINs and authorized roles when permitted
13. Click OK

VKEY: V0002473	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.126 DM2142: Remote access option

Description: The remote access option determines if connections to and from other Microsoft SQL Servers are allowed. Remote connections are used to support distributed queries and other data access and command executions across and between remote database hosts. The list of remote servers determines the servers that have defined for remote connections to and from the SQL Server instance. The list of remote logins determines which users on remote servers can connect to and from other SQL Servers. Remote servers and logins that are not properly secured can be used to compromise the server.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].dbo.sysconfigures
WHERE comment = 'allow remote access'
```

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'remote access'
```

If a value of 1 is returned for Config_Value, remote access is enabled.

If the use of linked servers is not documented and authorized in the System Security Plan and AIS Functional Architecture documentation, this is a Finding.

If the use of linked servers is not approved by the IAO, this is a Finding.

Note: See check DG0190 for authorized linked servers.

If remote access is not documented in the System Security Plan and AIS Functional Architecture documentation regardless of authorization or use, this is a Finding.

Fix:

Document remote access in the System Security Plan and AIS Functional Architecture documentation.

If required and authorized, document the requirement and authorization in the System Security Plan and AIS Functional Architecture documentation.

To enable remote access:

From the query prompt:

```
EXEC SP_CONFIGURE 'remote access', 1
RECONFIGURE
```

If not required, disable remote access and document the requirement and authorization in the System Security Plan and AIS Functional Architecture documentation.

To disable remote access:

From the query prompt:

```
EXEC SP_CONFIGURE 'remote access', 0
RECONFIGURE
```

Follow procedures documented on Microsoft's website on how to configure a remote server setup.

For SQL Server 2000:

http://msdn.microsoft.com/en-us/library/aa215388(SQL.80).aspx

For SQL Server 2005

http://support.microsoft.com/kb/914277

VKEY: V0002485	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0075: CAT II) The DBA will ensure database connections to remote databases or remote or external applications and services are disabled and/or not defined unless database replication is in use or the remote connection is mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.127 DM3566: Authentication mode

Description: SQL Server authentication does not provide a sufficiently robust password complexity and management capability to meet stringent security requirements. SQL Server allows use of Windows authentication, a more robust and security authentication service, to control access to the database.

Check:

From the query prompt:

```
EXEC XP_LOGINCONFIG 'login mode'
```

If a value of 'Windows Authentication' is returned for config_value, this is Not a Finding.

If a value of 'Mixed' is returned for config_value and the version is SQL Server 2005 or later on Windows 2003 Server or later, this is Not a Finding.

If a value of 'Mixed' is returned for config_value and the version is SQL Server 7/2000 on Windows 2003 or later, this is a Finding.

If Mixed mode is returned for SQL Server 2005 on Windows 2003 (or later combinations), confirm in the System Security Plan that SQL Server authentication is required and authorized. If it is not, this is a Finding.

Note: SQL Server authentication and the use of passwords are dependent on password management configured on the host platform. Sufficient password management is available only in SQL Server 2005 on Windows 2003 or later. Password authentication is discouraged and only authorized where Windows authentication is not possible.

Fix:

Configure the instance to accept Windows authentication only.

From the query prompt:

```
EXEC XP_LOGINCONFIG 'login mode', 1
```

If the SQL Server version is 2005 and the host Windows version is 2003 (or later versions of either), and SQL Server authentication is required and authorized, document the requirement with a justification in the System Security Plan.

VKEY: V0002487	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAIA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2			
STIG Requirement:	(DG0078: CAT II) The DBA will ensure database user accounts are configured to require individual authentication in order to connect to the DBMS.			

4.128 DM3763: CmdExec or ActiveScripting jobs

Description: SQL Server Agent CmdExec and ActiveScripting subsystems allow the execution of code by the host operating system under the security context. Allow use of these features only to SYSADMINs and use only where necessary to limit risk of database exploit to the host operating system. Members of the SYSADMIN group have access to all proxies and subsystems by default. Additional assignments are not necessary and would be considered suspect.

Check:

For SQL Server 7 & 2000:

From the SQL Server Enterprise Manager GUI:

1. Connect/expand SQL Server
2. Expand Management
3. Right-click on SQL Server Agent
4. Select Properties
5. Select Job System tab
6. View checkbox for 'Only users with SysAdmin privileges can execute CmdExec and ActiveScripting job steps'

If this box is not checked, this is a Finding.

Or

From the Windows registry editor, navigate to:

HKEY_LOCAL_MACHINE / SOFTWARE / MICROSOFT / MSSQLServer / SQLSERVERAGENT

Double click on the SYSAdminOnly Value. If the value is hex 1, this is Not a Finding.

If the value is hex 0, this is a finding. The key type should be REG_DWORD. If the key type is not correct, this should be marked as a finding.

From Windows:

Review the Windows account assigned to the SQL Server Agent service.

1. Click Start
2. Select Control Panel / Administrative Tools (Win2K) or Select Administrative Tools (Win2K3)
3. Click on Services
4. Locate the SQLServerAgent ([Instance Name]) service

5. Note the account in the Log On As column for the service

Review the SQL Server Agent account(s):

1. Click Start
2. Select Control Panel / Administrative Tools (Win2K) or Select Administrative Tools (Win2K3)
3. Click on Computer Management
4. Expand System Tools
5. Expand Local Users and Groups
6. Click on Groups
7. Double-click on the Administrators group

If the service account is a member of the Local Administrator's group, this is a Finding.

Note: If the service account is not a member of the Local Administrator's group, users who are not members of the SYSADMIN role cannot submit CmdExec or active scripting jobs to the Agent

For SQL Server 2005:

From the query prompt:

```
USE msdb
EXEC SP_ENUM_PROXY_FOR_SUBSYSTEM @subsystem_name =
'ActiveScripting'
EXEC SP_ENUM_PROXY_FOR_SUBSYSTEM @subsystem_name =
'CmdExec'
```

If no records are returned, this is Not a Finding.

For each proxy listed:

```
EXEC SP_ENUM_LOGIN_FOR_PROXY @proxy_name = '[proxy name]'
```

Replace [proxy name] with the proxy names returned above.

Review the names listed in the return. If any names include users that are not SYSADMINs or list groups that contain members other than SYSADMIN, this is a Finding.

Fix:

Members of the SYSADMIN role have access to all proxies by default. For any proxies defined for Active Scripting or CmdExec subsystems, remove all additional access privileges.

For SQL Server 7 & 2000:

From the SQL Server Enterprise Manager GUI:

1. Expand server
2. Expand Management
3. Right-click on SQLServer Agent
4. Select Properties
5. Select Job System tab
6. Select Non-SysAdmin job step proxy account / 'Only users with SysAdmin privileges can execute CmdExec and Active Scripting job steps'

For SQL Server 2005:

Select based on returns from the SP_ENUM_PROXY_SUBSYSTEM results:

From the query prompt:

```
EXEC SP_REVOKE_LOGIN_FROM_PROXY '[login name]' @proxy_name
= 'ActiveScripting'
EXEC SP_REVOKE_LOGIN_FROM_PROXY '[login name]' @proxy_name
= 'CmdExec'
```

Replace [login name] with the name returned in the SP_ENUM_PROXY_FOR_SUBSYSTEM procedure.

VKEY: V0002488	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA / ECLP	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0098: CAT II) The DBA will configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.129 DM3930: Error log retention

Description: For SQL Server, error logs are used to store system event and system error information. In addition to assisting in correcting system failures or issues that could affect system availability and operation, log information may also be useful in discovering evidence of malicious intent. Management of the error logs requires consideration and planning to prevent loss of security data and maintaining system operation.

Check:

Review the registry key value:

For SQL Server 7 & 2000:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ MSSQLServer \ MSSQLServer \ NumErrorLogs

For SQL Server 2005:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Microsoft SQL Server \ MSSQL.# \ MSSQLServer \ NumErrorLogs

where [#] indicates the sequence number assigned to the SQL Server instance.

Sequence number assignments to instances may be viewed at:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Microsoft SQL Server \ Instance Names \ SQL \[instance name]

Review the number assigned for the maximum number of error logs. Confirm this is the number documented in the System Security Plan.

If the number is not documented in the System Security Plan or the assigned value does not match the System Security Plan specification, this is a Finding.

Review evidence that error log retention is maintained for a minimum of one year. Error logs should be moved offline after 30 days or less depending on system storage capacity.

Fix:

Review the SQL Server error log usage and determine a strategy for maintenance.

The strategy should provide for the longest online retention that is considered meaningful and useful. This is determined over a period for operation and depends upon the amount of log data generated.

Error logs must be maintained for a minimum of one year (DG0030). Error logs should be moved offline to satisfy this retention requirement. Design the provision for evidence of retention and allow restoration (for review) of the error logs in the System Security Plan.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to and expand the SQL Server instance
2. Expand Management
3. Right-click on SQL Server Logs
4. Select Configure
5. Under the General Page, select or deselect Limit the number of error logs before they are recycled
6. Enter the number of error log files determined for the SQL Server instance
7. Click OK

VKEY: V0015137	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECCR	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.18			
STIG Requirement:	(DG0030: CAT II) The DBA will ensure the DBMS audit trail data is maintained for a minimum of one year.			

4.130 DM5267: Trace rollover on audit trace

Description: The majority of Microsoft SQL Server security auditing is provided by the trace facility. Traces may be created using system stored procedures or with Microsoft SQL Profiler. The trace must be running in order for security event data to be collected for analysis. Traces can specify a maximum size for the trace file. An action may also be specified when a maximum file size is reached. The trace file rollover option for a defined trace causes the current trace file to close and a new one to be opened with no loss of data. If a maximum file size has been set and the rollover option is not set, the trace stops writing when the maximum file size is reached. If the trace file writes function stops, then auditing is disabled.

Check:

If C2 Auditing is enabled (See Check DM0510**:** C2 audit mode), this check is Not a Finding.

Determine the SQL Server Edition:

From the query prompt:

```
SELECT CONVERT(INT, SERVERPROPERTY('EngineEdition'))
```

If value returned is 1 (Personal or Desktop Edition) or 4 (Express Edition), if auditing is not enabled or not configured completely to requirements, review the System Security Plan. If this is properly explained in the System Security Plan, this is Not a Finding. If this is not documented or documented poorly in the System Security Plan, this is a Finding.

If value returned is 2 (Standard Edition) or 3 (Enterprise/Developer Edition), these findings apply.

Determine if trace file rollover is enabled.

For SQL Server 2000:

From the query prompt:

```
SELECT traceid 'TraceID'
FROM ::FN_TRACE_GETINFO('0')
WHERE property = 1
AND value = 2
```

For SQL Server 2005:

From the query prompt:

```
SELECT traceid 'TraceID'
FROM ::FN_TRACE_GETINFO('0')
WHERE traceid <> 1 – Do not count default trace in SQL Server 2005
AND property = 1
AND value = 2
```

If no trace is returned, this is a Finding.

If the trace returned for Check DG0145 is not returned above, this is a Finding.

Fix:

Re-create the trace and specify TRACE_FILE_ROLLOVER (option = 2) added to SHUTDOWN_ON_ERROR (option = 4).

For SQL Server 2000:

From the query prompt:

```
EXEC SP_TRACE_CREATE [traceid] OUTPUT, 6, [tracefile], [maxfilesize],
NULL, [max # rollover files]
```

For SQL Server 2005:

From the query prompt:

```
EXEC SP_TRACE_CREATE [ @traceid = ] trace_id OUTPUT
, [ @options = ] option_value
, [ @tracefile = ] 'trace_file'
[ , [ @maxfilesize = ] max_file_size ]
[ , [ @stoptime = ] 'stop_time' ]
[ , [ @filecount = ] 'max_rollover_files' ]
```

VKEY: V0002500	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECRR	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.18			
STIG Requirement:	(DG0030: CAT II) The DBA will ensure the DBMS audit trail data is maintained for a minimum of one year.			

4.131 DM6015: Disable named pipes network protocol

Description: The named pipes network protocol requires more ports to be opened on firewalls than TCP/IP. Managing and administering multiple network protocols may unnecessarily complicate network controls.

Check:

For SQL Server 7 & 2000:

From the Windows registry editor:

HKEY_LOCAL_MACHINE \ Software \ Microsoft \ MSSQLServer \ MSSQLServer \ SuperSocketNetLib \ ProtocolList

Enabled = 'np' included in list.

If Named Pipes is enabled, this is a Finding.

For SQL Server 2005:

From the SQL Server Configuration Manager GUI:

1. Expand SQL Server 2005 Network Configuration
2. Repeat for each instance:
    a. Select Protocols for [instance name].
    b. View in the right pane, the status for Named Pipes

If Named Pipes is enabled, this is a Finding.

Fix:

If Named Pipes is required, document its use in the System Security Plan. Disable Named Pipes if not required and document this in the System Security Plan.

For SQL Server 7 & 2000:

From SQL Server Network Utility:

Under Enabled protocols:

1. Select Named Pipes
2. Click on Disable
3. Click OK (to save)
4. Click OK (to exit)

For SQL Server 2005:

From the SQL Server Configuration Manager GUI:

1. Expand SQL Server 2005 Network Configuration
2. Repeat for each instance:
    a. Select Protocols for [instance name]
    b. Double-click Named Pipes.
    c. Select No as the value for Enabled.
    d. Click OK
3. Click OK (acknowledge change won't take place until next restart)
4. Exit the SQL Server Configuration Manager GUI

VKEY: V0015124	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0103: CAT II) The DBA will ensure database and host system listeners that provide configuration of network restrictions are configured to restrict network connections to the database to authorized network addresses and protocols.			

4.132 DM6030: Event forwarding/Forward events setting

Description: If SQL Server is configured to forward events to an Alerts Management Server that is not available, then no alerts are issued for the server.

Check:

For SQL Server 7 & 2000:

From RegEdit, view the value:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ SQLServerAgent \ AlertForwardingServer

For SQL Server 2005:

From RegEdit, view values:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Sever \ MSSQL.[#] \ SQLServerAgent \ AlertForwardingServer

If the value is empty or NULL, this is Not a Finding.

If the value is not NULL, verify that the use of alert forwarding is authorized in the System Security Plan.

If alert forwarding is in use and not authorized and documented, this is a Finding.

Fix:

Enable use of event forwarding only as part of a SQL Server automated management system design where careful consideration and the requirements for its use are carefully considered. The plan should include consideration for network or alert management server failure and subsequent loss of alert data.

Include the alert management plan or a reference to it in the System Security Plan that includes the instance of SQL Server under review.

Disable event forwarding where not required.

For SQL Server 7 & 2000:

From the SQL Server Enterprise Manager GUI:

1. Expand instance
2. Right-click on SQL Server Agent
3. Select Properties
4. Select the Advanced page

5. Click on Forward events to a different server to remove the check from the check box.
6. Click the OK button to save and close

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Expand instance
2. Right-click on SQL Server Agent
3. Select Properties
4. Select the Advanced page
5. Click on Forward events to a different server to remove the check from the check box
6. Click the OK button to save and close

VKEY: V0015176	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0075: CAT II) The DBA will ensure database connections to remote databases or remote or external applications and services are disabled and/or not defined unless database replication is in use or the remote connection is mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.133 DM6045: SQL Server Agent permissions to proxies

Description: Database accounts granted access to SQL Server Agent proxies are granted permissions to create and submit specific function job steps to be executed by SQL Server Agent. Unauthorized users may use access to proxies to execute unauthorized functions against the SQL Server instance or host operating system.

Check:

Note: Access to ActiveScripting and CmdExec proxies is covered in check DM3763

For SQL Server 2005:

From the query prompt:

```
USE msdb
EXEC SP_ENUM_PROXY_FOR_SUBSYSTEM
```

If no records are returned, this is Not a Finding.

For each proxy listed that is not for CmdExec or ActiveScripting subsystems (checked under DM3763):

From the query prompt:

```
EXEC SP_ENUM_LOGIN_FOR_PROXY @proxy_name = '[proxy name]'
```

Replace [proxy name] with the proxy name returned above.

Review the names listed in the return.

Verify in the System Security Plan that any accounts or groups listed are authorized to access the proxy listed. If any are not, this is a Finding.

Fix:

Note: SYSADMINs have access to all proxies by default.

For SQL Server 2005:

For each user or group granted unauthorized access to a proxy (select based on returns from the SP_ENUM_PROXY_FOR_SUBSYSTEM results):

From the query prompt:

```
EXEC SP_REVOKE_LOGIN_FROM_PROXY '[login name]' @proxy_name
= '[proxy name]'
```

Replace [proxy name] with the name of the proxy and replace [login name] with the name returned in the SP_ENUM_PROXY_FOR_SUBSYSTEM procedure.

VKEY: V0015125	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAN	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0122: CAT II) The DBA will ensure all access to sensitive administrative DBMS data stored inside the database and in external host files is granted only to DBA and other authorized administrative database and OS accounts.			

4.134 DM6065: SQL Server replication agent accounts

Description: Use of shared accounts used by replication agents require that all permissions required to support each of the separate replication agent roles (snapshot publication, distribution, log reading, merge publication, queue reading, and replication maintenance) be assigned to the shared account. This translates to excess privilege assignment to the account to perform a specific job task and an exploit to the single account means a compromise to all replication elements accessed by the shared account. Separation of duties by use of separate and dedicated accounts reduces the risk to the entire replication implementation.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT c.credential_identity, p.name
FROM [master].sys.credentials c, [msdb].dbo.sysproxies p,
[msdb].dbo.sysproxysubsystem s
WHERE c.credential_id = p.credential_id
AND s.proxy_id = p.proxy_id
AND s.subsystem_id > 3
AND s.subsystem_id < 9
ORDER BY c.credential_identity, p.name
```

If any proxies are not assigned unique credential identities, this is a Finding.

Fix:

Create individual Windows accounts for each replication agent.

Specify the Windows account created for the replication agent, in the Replication Agent Security settings in SQL Server.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Expand instance
2. Expand Replication
3. Expand Local Publications
4. For each Local Publication:
    a. Right-click on the publication
    b. Select Properties
    c. Select Agent Security page
    d. Click on Security Settings button
    e. Enter the dedicated Windows account for the Snapshot Agent

f. Select Connect to the Publisher - By impersonating the process account
g. Click OK
h. Click OK

VKEY: V0015113	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Auto	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0102: CAT II) The DBA will ensure each database service or process runs under a custom, dedicated OS account that is assigned the minimum privileges required for operation where applicable.			

4.135 DM6070: Replication administration role privileges

Description: Role privileges required by replication include full privileges to the databases with replicated objects. Restrict replication database db_owner role memberships and the system distribution database replmonitor database role membership to authorized replication agent accounts that require access to the database. Unauthorized access can provide unintentional or malicious users greater opportunity to exploit replication access.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT COUNT(name)
FROM [master].dbo.sysdatabases
WHERE name = 'distribution'
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

If count = 0, the distribution database does not exist and this check is Not a Finding.

From the query prompt:

```
USE distribution
EXEC SP_HELPLROLEMEMBER 'replmonitor'
```

View the list of databases participating in replication:

```
EXEC SP_HELPREPLICATIONDBOPTION
```

For each replication database:

```
USE [database name]
EXEC SP_HELPROLEMEMBER 'db_owner'
```

If any role members listed are not authorized for replication access in the System Security Plan, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT COUNT(name)
FROM [master].sys.databases
WHERE name = 'distribution'
```

```
AND state = 0
```

If count = 0, the distribution database does not exist and this check is Not a Finding.

From the query prompt:

```
USE distribution
EXEC SP_HELPROLEMEMBER 'replmonitor'
```

View list of databases participating in replication:

```
EXEC SP_HELPREPLICATIONDBOPTION
```

For each replication database:

```
USE [database name]
EXEC SP_HELPROLEMEMBER 'db_owner'
```

If any role members listed are not authorized for replication access in the System Security Plan, this is a Finding.

Fix:

Revoke role membership for unauthorized accounts granted replication role memberships:

```
USE [database name]
EXEC SP_DROPROLEMEMBER '[replmonitor or db_owner]' FROM '[account name]'
```

VKEY: V0015178	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0085: CAT II) The DBA will ensure the minimum database administrative privileges are assigned to database administrative roles to perform the administrative job function.			

4.136 DM6075: Replication snapshot folder protection

Description: Replication snapshot folders contain database data to which only authorized replication accounts require access. Unauthorized access to these folders could compromise data confidentiality and integrity, and could compromise database availability.

Check:

For SQL Server 2005:

View the list of databases participating in replication:

EXEC SP_HELPREPLICATIONDBOPTION

For each replication database:

EXEC SP_HELPPUBLICATION

If snapshot_in_defaultfolder is 1 for any records returned, the snapshot folder name is:

[install dir]\[instance dir]\MSSQL\ReplData

If the snapshot_in_defaultfolder is 0, then the snapshot folder name is listed in alt_snapshot_folder.

View OS permissions to the snapshot folder:

Review operating system permissions assigned to the snapshot folder using Windows Explorer.

The following are required/authorized permissions by role:

1. Administrators/DBAs: Full Control
2. Snapshot Agents: Write access
3. Merge and Distribution agents: Read access

If any permission other than those listed is assigned or are assigned to unauthorized accounts, this is a Finding.

View database permissions to the snapshot folder:

For each replication database:

EXEC SP_HELPPUBLICATION_SNAPSHOT '[publication name]'

If any permission is granted to accounts other than Administrators, DBAs, CREATOR OWNER, SYSTEM, or the snapshot agent account, merge, or distribution agents, this is a Finding.

If merge and distribution agents have more than Read access to the snapshot folder, this is a Finding.

Fix:

For SQL Server 2005:

Restrict access to the replication snapshot folders:

From Windows Explorer:

1. Administrators/DBAs: Full Control
2. Snapshot Agents: Write access
3. Merge, Subscription, and Distribution agents: Read access

VKEY: V0015182	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAN	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0123: CAT II) The DBA will ensure all access to sensitive application data stored inside the database, and in external host files, is granted only to database accounts and OS accounts in accordance with user functions as specified by the Information Owner.			

4.137 DM6085: Analysis Services ad hoc data mining queries

Description: SQL Server Ad Hoc distributed queries allow specific functions (OPENROWSET and OPENDATASOURCE) to connect to remote systems without those remote systems being defined within database. Access to unauthorized systems could lead to unauthorized activity in remote systems that could compromise the local database.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for DataMining \ AllowAdHocOpenRowsetQueries

If value = 'true', this is a Finding.

The AllowAdHocOpenRowsetQueries value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[AllowAdHocOpenRowsetQueries]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

Set value for AllowAdHocOpenRowsetQueries to 'false'

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for DataMining \ AllowAdHocOpenRowsetQueries

5. Select value = 'false'
6. Click OK

VKEY: V0015183	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0075: CAT II) The DBA will ensure database connections to remote databases or remote or external applications and services are disabled and/or not defined unless database replication is in use or the remote connection is mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.138 DM6086: Analysis Services anonymous connections

Description: Anonymous connections allow unauthenticated access to the database. Although the database may not store sensitive application data, operation and data compromise may occur without accountability where unauthenticated access is allowed.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ RequireClientAuthentication

If value = 'false', this is a Finding.

The RequireClientAuthentication value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[RequireClientAuthentication]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

Set value for RequireClientAuthentication to 'true'

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ RequireClientAuthentication
5. Select value = 'true'
6. Click OK

VKEY: V0015184	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: IAIA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2			
STIG Requirement:	(DG0078: CAT II) The DBA will ensure database user accounts are configured to require individual authentication in order to connect to the DBMS.			

4.139 DM6087: Analysis Services links to objects

Description: Analysis Services may make connections to external SQL Server instances. In some cases this may be required for the intended operation, however, where not required, this may introduce unnecessary risk where unauthorized external links may be made.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

If the System Security Plan indicates Links to Other instances is required for operation, this check is Not a Finding.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Feature \ LinkToOtherInstanceEnabled

If the value = 'true', this is a Finding.

The LinkToOtherInstanceEnabled value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[LinkToOtherInstanceEnabled]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

Set value for LinkToOtherInstanceEnabled to 'false'.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance

3. Select Properties
4. View the value listed for Feature \ LinkToOtherInstanceEnabled
5. Select value = 'false'
6. Click OK

VKEY: V0015204	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0098: CAT II) The DBA will configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.140 DM6088: Analysis Services links from objects

Description: Analysis Services allows other server instances to link to local analysis services objects. Where not required, enabling of this allowance can unnecessarily expose the database objects to unauthorized access or compromise.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

If the System Security Plan indicates Links from Other instances is required for operation, this check is Not a Finding.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Feature \ LinkFromOtherInstanceEnabled

If the value = 'true', this is a Finding.

The LinkFromOtherInstanceEnabled value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[LinkFromOtherInstanceEnabled]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

Set value for LinkFromOtherInstanceEnabled to 'false'.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties

4. View the value listed for Feature \ LinkFromOtherInstanceEnabled
5. Select value = 'false'
6. Click OK

VKEY: V0015186	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0098: CAT II) The DBA will configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.141 DM6099: Analysis Services user-defined COM functions

Description: Allowing user-defined COM functions can allow unauthorized code access to the Analysis Services instance. Where not required as part of the operational design, allowing user-defined COM functions can expose the instance to unnecessary risk.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

If the System Security Plan indicates User-Defined COM Functions is required for operation, this check is Not a Finding.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Feature \ ComUdfEnabled

If the value = 'true', this is a Finding.

The User-Defined COM Functions value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[ComUdfEnabled]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

If not documented as required and authorized by the IAO, set value for ComUdfEnabled to 'false'.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance

3. Select Properties
4. View the value listed for Feature \ ComUdfEnabled
5. Select value = 'false'
6. Click OK

VKEY: V0015181	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation			

4.142 DM6101: Analysis Services required protection level

Description: Sensitive data is vulnerable to unauthorized access when traversing untrusted network segments. Encryption of the data in transit helps protect the confidentiality of the data.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ DataProtection \ RequiredProtectionLevel

If the value <> '1', this is a Finding.

The RequiredProtectionLevel value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[DataProtection][RequiredProtectionLevel]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

Set DataProtection\RequiredProtectionLevel to use encryption.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ DataProtection \ RequiredProtectionLevel

5. Select value = '1'
6. Click OK

VKEY: V0015188	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECCT	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.6			
STIG Requirement:	(DG0167: CAT I) The DBA will ensure database communications are encrypted when transmitting sensitive data across untrusted network segments and in accordance with the application requirements.			

4.143 DM6102: Analysis Services required web protection level

Description: Sensitive data crossing untrusted network segments is vulnerable to unauthorized access. Encryption helps protect sensitive data in transit from unauthorized access.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ DataProtection \ RequiredProtectionLevel

If the property is not listed, this check is Not a Finding.

If the value <> '1', this is a Finding.

The DataProtection \ RequiredWebProtectionLevel value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[DataProtection][RequiredWebProtectionLevel]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

Set DataProtection\RequiredWebProtectionLevel to use encryption.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties

4. View the value listed for Security \ DataProtection \ RequiredWebProtectionLevel
5. Select value = '1'
6. Click OK

VKEY: V0015189	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECCT	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.6			
STIG Requirement:	(DG0167: CAT I) The DBA will ensure database communications are encrypted when transmitting sensitive data across untrusted network segments and in accordance with the application requirements			

4.144 DM6103: Analysis Services security package list

Description: Analysis Services Security Packages are security applications provided outside of the default Analysis Services installation. The packages may be provided by custom development or commercial third-party products used for client authentication. Use of untested or unverified security applications may introduce unknown vulnerabilities to the instance. Restrict use of non-default security packages to tested and trusted applications that meet DOD authentication requirements.

Check:

For SQL Server 2005:

If Analysis Services is not installed on the local host, this check is Not a Finding.

Note: To detect installation, view the Windows Services snap-in. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ SecurityPackageList

If the value is not NULL and lists packages other than those documented in the System Security Plan, this is a Finding.

The SecurityPackageList value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[SecurityPackageList]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ SecurityPackageList
5. Select value and delete all unauthorized packages from the list

6. Click OK

VKEY: V0015190	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0098: CAT II) The DBA will configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.145 DM6106: Analysis Services administrative data protection

Description: Administrative data that may contain sensitive configuration, operational, or other sensitive data is vulnerable to unauthorized access when traversing untrusted network segments. Encryption of the data in transit helps protect the confidentiality of the data.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ AdministrativeDataProtection \ RequiredWebProtectionLevel

If the value <> '1', this is a Finding.

The AdministrativeDataProtection \ RequiredWebProtectionLevel value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[DataProtection][RequiredWebProtectionLevel]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

Set AdministrativeDataProtection \ RequiredWebProtectionLevel to use encryption.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance

3. Select Properties
4. View the value listed for Security \ AdministrativeDataProtection \ RequiredWebProtectionLevel
5. Select value = '1'
6. Click OK

VKEY: V0015191	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECCT	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.6			
STIG Requirement:	(DG0167: CAT I) The DBA will ensure database communications are encrypted when transmitting sensitive data across untrusted network segments and in accordance with the application requirements			

4.146 DM6107: Analysis Services data protection

Description: Administrative data that may contain sensitive configuration, operational, or other sensitive data is vulnerable to unauthorized access when traversing untrusted network segments. Encryption of the data in transit helps protect the confidentiality of the data.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. View the value listed for Security \ DataProtection \ RequiredProtectionLevel

If the value <> '1', this is a Finding.

The DataProtection\RequiredProtectionLevel value may also be viewed in the Analysis Services configuration file, msmdsrv.ini under XML tag:

[DataProtection][RequiredProtectionLevel]

The configuration file may be found in the [install dir] \ MSSQL.[#] \ OLAP \ Config directory.

Fix:

Set DataProtection \ RequiredProtectionLevel to use encryption.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties

4. View the value listed for Security \ AdministrativeDataProtection \ RequiredProtectionLevel
5. Select value = '1'
6. Click OK

VKEY: V0015192	Severity: CAT 1		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECCT	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.6			
STIG Requirement:	(DG0167: CAT I) The DBA will ensure database communications are encrypted when transmitting sensitive data across untrusted network segments and in accordance with the application requirements			

4.147 DM6108: Analysis Services server role membership

Description: The Analysis Services server role grants server-wide security privileges to the assigned user. An unauthorized user could compromise database and analysis server data and operational integrity or availability.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. Select the Security page
5. View member names assigned to the server role

If any assigned members are not included as authorized in the System Security Plan, this is a Finding.

Fix:

Remove unauthorized members from the Analysis Service instance.

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Select Properties
4. Select the Security page
5. Select any unauthorized user to remove
6. Click the Remove button
7. Click OK

VKEY: V0015193	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECLP	Check Type: Manual	Database Level: False	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.11.2			
STIG Requirement:	(DG0116: CAT II) The IAO will ensure database privileged role assignments are restricted to IAO-authorized accounts.			

4.148 DM6109: Analysis Services database role membership

Description: Unauthorized group membership assignment grants unauthorized privileges to database accounts. Unauthorized may lead to a compromise of data confidentiality or integrity.

Check:

For SQL Server 2005:

If Analysis Services is not deployed on the local host, this check is Not a Finding.

Note: To detect deployment, view Windows Services. If SQL Server Analysis Services ([instance name]) is not listed, then Analysis Services is not installed on this host.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Right click on the Analysis Services instance
3. Expand Databases
4. Repeat for each database:
   a. Click on each database role
   b. View the member list

If any members are assigned database roles that are not documented in the System Security Plan, this is a Finding.

Fix:

For SQL Server 2005:

Authorize and document all Analysis Services database role assignments in the System Security Plan.

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. Expand the Analysis Services instance
3. Expand Databases
4. Repeat for each database:
   a. Click on each database role
   b. Open the member list
   c. Select any unauthorized users
   d. Click the Remove button
   e. Click OK

VKEY: V0015194	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECAN	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0123: CAT II) The DBA will ensure all access to sensitive application data stored inside the database, and in external host files, is granted only to database accounts and OS accounts in accordance with user functions as specified by the Information Owner.			

4.149 DM6120: Reporting Services web service requests and HTTP

Description: Where not required, SOAP and URL access to the web service unnecessarily exposes the report server to attack via the SOAP and HTTP protocols.

Check:

For SQL Server 2005:

If Reporting Services is not installed, this check is Not a Finding.

Note: To detect installation, view Windows Services. If SQL Server Reporting Services ([instance name]) is not listed, then Reporting Services is not installed on this host.

From Surface Area Configuration for Features:

1. Connect to the Report Services instance
2. Expand the instance
3. Expand Report Services
4. Select Web Service Requests and HTTP Access

If checked, verify that Web Service requests are HTTP access are required and the requirement is documented in the System Security Plan. If it is not, this is a Finding.

Fix:

Document requirements for enabling Report Services access via web services and HTTP. If not required, disable Web Service Requests and HTTP access.

For SQL Server 2005:

From Surface Area Configuration for Features:

1. Connect to the Report Services instance
2. Expand the instance
3. Expand Report Services
4. Select Web Service Requests and HTTP Access
5. Click on Enable Web Service Requests and HTTP access to clear the check box
6. Click OK

VKEY: V0015199	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0016: CAT III) The DBA will ensure unused optional database components or features, applications, and objects are removed from the database and host system. If the optional component cannot be uninstalled or removed, then the DBA will ensure the unused component or feature is disabled.			

4.150 DM6121: Reporting Services scheduled events and report

Description: Where not required, Scheduled events and report delivery unnecessarily exposes the report server to attack via Report Service event handling and report delivery.

Check:

For SQL Server 2005:

If Reporting Services is not installed, this check is Not a Finding.

Note: To detect installation, view Windows Services. If SQL Server Reporting Services ([instance name]) is not listed, then Reporting Services is not installed on this host.

From Surface Area Configuration for Features:

1. Connect to the Report Services instance
2. Expand the instance
3. Expand Report Services
4. Select Scheduled events and report delivery

If checked, verify that Scheduled events and report delivery is required and the requirement is documented in the System Security Plan. If it is not, this is a Finding.

Fix:

Document requirements for enabling 'Report Services Scheduled events and report delivery'. If not required, disable Scheduled events and report delivery.

For SQL Server 2005:

From Surface Area Configuration for Features:

1. Connect to the Report Services instance
2. Expand the instance
3. Expand Report Services
4. Select Scheduled events and report delivery
5. Click on the Scheduled events and report delivery to clear the check box
6. Click OK

VKEY: V0015205	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0016: CAT III) The DBA will ensure unused optional database components or features, applications, and objects are removed from the database and host system. If the optional component cannot be uninstalled or removed, then the DBA will ensure the unused component or feature is disabled.			

4.151 DM6122: Reporting Services Windows integrated security

Description: Use of Windows integrated security may allow access via Report Services bypasses security controls assessed at the database level. This may be restricted by requiring that all report data source connections use specific credentials to access report data sources.

Check:

For SQL Server 2005:

If Reporting Services is not installed, this check is Not a Finding.

Note: To detect installation, view Windows Services. If SQL Server Reporting Services ([instance name]) is not listed, then Reporting Services is not installed on this host.

From Surface Area Configuration for Features:

1. Connect to the Report Services instance
2. Expand the instance
3. Expand Report Services
4. Select Windows Integrated Security

If checked, this is a Finding.

Fix:

For SQL Server 2005:

Disable Windows Integrated Security.

From Surface Area Configuration for Features:

1. Connect to the Report Services instance
2. Expand the instance
3. Expand Report Services
4. Select Windows Integrated Security
5. Click on Windows Integrated Security to clear the check box
6. Click OK

VKEY: V0015203	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: IAIA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.2			
STIG Requirement:	(DG0078: CAT II) The DBA will ensure database user accounts are configured to require individual authentication in order to connect to the DBMS.			

4.152 DM6123: clr_enabled parameter

Description: The clr_enabled parameter configures SQL Server to allow or disallow use of Command Language Runtime objects. CLR objects is managed code that integrates with the .NET Framework. This is a more secure method than external stored procedures, although it still contains some risk. Where no external application execution requirements are required, disallowing use of any improves the overall security posture of the database.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'clr enabled'
```

If the value of Config_Value is 0, this is Not a Finding.

If the value of Config_Value is 1, confirm in the System Security Plan that access to CLR applications is required. If it is not, this is a Finding.

Fix:

Where CLR object use is part of the designed and approved use of the SQL Server database, document the requirement in the System Security Plan.

Where CLR object use is not required, disable its use.

For SQL Server 2005:

From the query prompt:

```
EXEC SP_CONFIGURE 'clr_enabled', 0
RECONFIGURE
```

VKEY: V0015202	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0016: CAT III) The DBA will ensure unused optional database components or features, applications, and objects are removed from the database and host system. If the optional component cannot be uninstalled or removed, then the DBA will ensure the unused component or feature is disabled.			

4.153 DM6126: XML web service access

Description: XML Web Service endpoints expose the database its data to web service access. Where not carefully designed and implemented, web services can unnecessarily expose the database to additional exploit that compromises data confidentiality and integrity. Removing web service endpoints helps to protect the database from unauthorized web service access.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.http_endpoints
WHERE (is_integrated_auth_enabled = 0
 AND is_kerberos_auth_enabled = 0
 AND is_ntlm_auth_enabled = 0)
AND state = 0
ORDER BY name
```

Review the list of any endpoints returned. If no records are returned, this is Not a Finding.

If any endpoints are returned and not listed as a required and authorized XML web service endpoint in the System Security Plan and AIS Functional Architecture documentation, this is a Finding.

If listed endpoints are:

1. Not using integrated authentication (is_integrated_auth_enabled = 0)
2. Not using Kerberos authentication (is_kerberos_auth_enabled = 0) and
3. Not using NT LAN Manager (NTLM) authentication (is_ntlm_auth_enabled = 0)
4. Are STARTED, listening and processing requests (state = 0)

this is a Finding.

If listed endpoints are required to use SSL (is_ssl_port_enabled = 1 and is_clear_port_enabled = 0) and are not, this is a Finding.

If listed endpoints are enabled to use anonymous access (is_anonymous_enabled = 1) and is not documented and authorized, this is a Finding.

Fix:

For SQL Server 2005:

Authorized and document XML web service endpoints in the System Security Plan and AIS Functional Architecture documentation. Where not authorized, drop XML web service endpoints.

From the query prompt:

DROP ENDPOINT [endpoint name]

Where documented and authorized, set each endpoint to use the appropriate authentication protocol, SSL if required and disable anonymous access if not authorized. If a clear port is also required and authorized, ensure the value for clear_port is set to a known value (i.e. HTTP port 80 or other IAO authorized port value).

VKEY: V0015206	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0075: CAT II) The DBA will ensure database connections to remote databases or remote or external applications and services are disabled and/or not defined unless database replication is in use or the remote connection is mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.154 DM6128: Service broker access

Description: Service Broker endpoints expose the database to SQL Server messaging communication access. Where not carefully designed and implemented, messaging communication can unnecessarily expose the database to additional exploit that compromises data confidentiality and integrity. Removing messaging communication endpoints helps to protect the database from unauthorized messaging communication access.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name FROM [master].sys.service_broker_endpoints
```

Review the list of any endpoints returned. If no records are returned, this is Not a Finding.

If any endpoints are returned and are not listed as a required and authorized XML web service endpoint in the System Security Plan, this is a Finding.

Fix:

For SQL Server 2005:

Authorize and document Service Broker endpoints in the System Security Plan. Where not authorized, drop Service Broker service endpoints.

From the query prompt:

```
DROP ENDPOINT [endpoint name]
```

VKEY: V0015165	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0075: CAT II) The DBA will ensure database connections to remote databases or remote or external applications and services are disabled and/or not defined unless database replication is in use or the remote connection is mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.155 DM6130: Web assistant procedures option

Description: The Web Assistant procedures are used by database applications to create web pages. This capability may easily be abused to send malicious messages to remote users or systems. Disabling its use helps to protect the database from generating or receiving malicious email notifications.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'web assistant procedures'
```

If the value of Config_Value is 1, confirm in the System Security Plan and AIS Functional Architecture documentation that Web Assistant procedures are required and approved by the IAO. If it is not documented, required and approved, this is a Finding.

Fix:

Authorize and document requirements for use of Web Assistant Procedures in the System Security Plan and AIS Functional Architecture documentation. Where not authorized, disable use of Web Assistant Procedures.

For SQL Server 2005:

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'Web Assistant procedures', 0
RECONFIGURE
```

VKEY: V0015198	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.156 DM6140: SQL Server Agent dedicated proxy accounts

Description: SQL Server proxies use to execute specific job functions defined for SQL Server Agent. If proxies share a single account for multiple job functions, least privileges cannot be assigned based on the particular job function. This can compromise the security of the shared functions should a compromise of the SQL Server Agent job occur.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT c.credential_identity, p.name
FROM [master].sys.credentials c, [msdb].dbo.sysproxies p,
[msdb].dbo.sysproxysubsystem s
WHERE c.credential_id = p.credential_id
AND s.proxy_id = p.proxy_id
AND s.subsystem_id < 4
AND s.subsystem_id > 8
ORDER BY c.credential_identity, p.name
```

Review the list of proxies and assigned logins.

If any login names are listed more than once, this is a Finding.

Fix:

For SQL Server 2005:

Create Windows accounts for each proxy defined.

Assign only the file permissions, subsystem access and other privileges required to run the SQL Server Agent job.

VKEY: V0015197	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAN	Check Type: Auto	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0122: CAT II) The DBA will ensure all access to sensitive administrative DBMS data stored inside the database and in external host files is granted only to DBA and other authorized administrative database and OS accounts.			

4.157 DM6145: Proxy account subsystem privileges

Description: SQL Server subsystems define a set of functionality available for assignment to a SQL Server Agent proxy. These act as privileges to perform certain job tasks. Excess privilege assignment or subsystem assignment can lead to unauthorized access to the SQL Server instance or host operating system.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT p.name, sp.subsystem
FROM [msdb].dbo.sysproxies p, [msdb].dbo.sysproxysubsystem s,
[msdb].dbo.syssubsystems sp
WHERE p.proxy_id = s.proxy_id
AND s.subsystem_id = sp.subsystem_id
ORDER BY p.name, sp.subsystem
```

Review the list of subsystem assignments to proxies against the authorized list in the System Security Plan document. If unauthorized subsystems are assigned to any proxy or is not documented, this is a Finding.

Fix:

For SQL Server 2005:

Define and document in the System Security Plan the minimum subsystem assignments required by individual proxies.

Assign to each proxy only those subsystems required to complete the SQL Server Agent job.

VKEY: V0015196	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAN	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0122: CAT II) The DBA will ensure all access to sensitive administrative DBMS data stored inside the database and in external host files is granted only to DBA and other authorized administrative database and OS accounts.			

4.158 DM6150: Cross db ownership chaining option

Description: Cross database ownership chaining allows permissions to objects to be assigned by users other than the Information Owner. This allows access to objects that are not authorized directly by the Information Owner based on job functions defined by the owner. Unauthorized access may lead to a compromise of data integrity or confidentiality.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'cross db ownership chaining'
```

If the value of Config_Value is 0, this is Not a Finding.

If the value of Config_Value is 1, confirm in the System Security Plan that this option is documented, required and approved by the IAO. If it is not documented, required and approved, this is a Finding.

Fix:

For SQL Server 2005:

Authorize and document requirements for use of cross db ownership chaining in the System Security Plan and AIS Functional Architecture documentation. Where not authorized, disable its use.

From the query prompt:

```
EXEC SP_CONFIGURE 'cross db ownership chaining', 0
RECONFIGURE
```

VKEY: V0015201	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0121: CAT II) The DBA will ensure database privileges are assigned via roles and not directly assigned to database accounts. Privileges may be assigned directly to application owner accounts where the DBMS does not otherwise support access via roles.			

4.159 DM6155: DisallowAdhocAccess for providers

Description: Ad hoc access allows undefined access to remote systems. Access to remote systems should be controlled to prevent untrusted data to be executed or uploaded to the local server.

Check:

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Expand Database
2. Expand Server Objects
3. Expand Linked Servers
4. Expand Providers
5. For each Provider listed:
    a. Right click on Provider name
    b. Click Properties
    c. View Provider options

If "Disallow adhoc access" is not enabled (checked) for all Providers, this is a Finding.

Fix:

For SQL Server 2005:

Enable Disallow adhoc access for all linked servers.

From the SQL Server Management Studio GUI:

1. Expand Database
2. Expand Server Objects
3. Expand Linked Servers
4. Expand Providers
5. For each Provider listed:
    a. Right click on Provider name
    b. Select Properties
    c. Click on the Enable check box for Name = Disallow adhoc access
    d. Click OK button

Note: The procedure described above will disallow adhoc access for all linked servers that use the providers.

VKEY: V0015187	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0098: CAT II) The DBA will configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.160 DM6160: Ad hoc distributed queries option

Description: Adhoc queries allow undefined access to remote database sources. Access to untrusted databases could result in execution of malicious applications and/or a compromise of local data confidentiality and integrity.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'ad hoc distributed queries'
```

If the value of Config_Value is 0, this is Not a Finding.

If the value of Config_Value is 1, confirm in the System Security Plan that this option is documented, required and approved by the IAO. If it is not documented, required and approved, this is a Finding.

Fix:

For SQL Server 2005:

Authorize and document requirements for use of Ad hoc distributed queries in the System Security Plan and AIS Functional Architecture documentation. Where not authorized, disable its use.

From the query prompt:

```
EXEC SP_CONFIGURE 'remote admin connections', 0
RECONFIGURE
```

VKEY: V0015166	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0098: CAT II) The DBA will configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.161 DM6189: Dedicated data file directories

Description: Data directories require different access controls than software file directories. Locating data directories in separate directories on a dedicated disk partition allows assign of access controls to only those users that require access and helps protect the data from unauthorized access.

Check:

For SQL Server 7 & 2000:

Review the default data and log directory specifications:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ MSSQLServer \ DefaultData
HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ MSSQLServer \ MSSQLServer \ DefaultLog

If the DefaultData directory lists the same directory as the DefaultLog directory, this is a Finding.

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
SELECT name, filename
FROM sysfiles
ORDER BY name
```

If the files from the master database indicate the same directory as any other database files, this is a Finding.

If any results show more than one database using the same physical filename, this is a Finding.

If any directories that contain data (*.MDF) and transactional log files (*.LDF) contain any other files other than *.MDF and *.LDF files, this is a Finding.

If any databases share the same directory, then verify in the System Security Plan that the databases are shared by the same application. If they are not, this is a Finding.

For SQL Server 2005:

Review the default data and log directory specifications:

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ MSSQLServer \ DefaultData
HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Microsoft SQL Server \ MSSQL.[#] \ MSSQLServer \ DefaultLog

If the DefaultData directory lists the same directory as the DefaultLog directory, this is a Finding.

Review the master database file locations:

From the query prompt:

```
SELECT physical_name, type_desc
FROM [master].sys.master_files
ORDER BY physical_name
```

If any results show more than one database using the same physical filename, this is a Finding.

If any files from either the master_files or database_files show log files (*_log.ldf files) in the same directory as data files, this is a Finding.

Note: Transactional log files (*.LDF) files can coexist with data files (*.MDF). A transactional log files will have a similar name or a variant name of its matching data file (ex: master.mdf vs. mastlog.ldf). Not all data files will have a corresponding transactional log file.

If any databases share the same directory, then verify in the System Security Plan that the databases are shared by the same application. If they are not, this is a Finding.

Fix:

Create at least one dedicated disk partition to store database data and log files.

Create dedicated directories to store database data files for each individual application that uses the database.

Include a dedicated directory for the Master database data files.

Specify the dedicated database data file disk partition for the default data directory.

Include this information in the System Security Plan and AIS Functional Architecture documentation.

VKEY: V0015167	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: DCPA	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.6			
STIG Requirement:	(DG0111: CAT II) The DBA will install and maintain database data directories including transaction log and audit files in dedicated directories or disk partitions separate from software or other application files.			

4.162 DM6193: Analysis Services permissions to data sources

Description: Access control applied to data sources controls user access to remotely defined systems using the authentication and authorizations defined for the data source. Unauthorized access to the data source in turn provides unauthorized access to remote systems.

Check:

For SQL Server 2005:

From the SQL Server Management Studio GUI:

1. Connect to the Analysis Services instance
2. For each Analysis Services database:
    a. Expand the database
    b. Expand Roles
    c. For each role listed:
        i. Right-click on the role
        ii. Select Properties
        iii. Select the Data Sources page

Review the list of data sources listed for the role against authorized roles in the System Security Plan.

If access to any unauthorized data sources is assigned to the role, this is a Finding.

If documentation does not exist or is insufficient to determine authorized access, this is a Finding.

Fix:

For SQL Server 2005:

Document all roles authorized to access data sources in the System Security Plan. Remove any unauthorized data sources from roles.

VKEY: V0015180	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECAN	Check Type: Manual	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0122: CAT II) The DBA will ensure all access to sensitive administrative DBMS data stored inside the database and in external host files is granted only to DBA and other authorized administrative database and OS accounts.			

4.163 DM6195: Database TRUSTWORTHY status

Description: The TRUSTWORTHY database setting restricts access to database resources by databases that contain assemblies with the EXTERNAL_ACCESS or UNSAFE permission settings and modules that use impersonation of accounts assigned elevated privileges. Unless all assemblies and code for the database have been reviewed, especially in the case where databases have been detached and attached between server instances, leaving the TRUSTWORTHY status to off can help reduce threats from malicious assemblies or modules.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE is_trustworthy_on = 1
AND name <> 'msdb'
AND state = 0
```

If any database names are returned, then verify in the System Security Plan that the TRUSTWORTHY database setting is documented as required and authorized.

If it is not documented, required and authorized, this is a Finding.

Fix:

Disable TRUSTWORTHY status on all databases (except the msdb database) if enabled and not authorized

For SQL Server 2005:

From the query prompt:

```
ALTER DATABASE [database name] SET TRUSTWORTHY OFF
```

Include in the System Security Plan all relevant settings for each database.

VKEY: V0015173	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0063: CAT II) The DBA will restrict restore permissions on databases to DBAs and/or the database owners.			

4.164 DM6198: Agent XPs option

Description: The Agent XPs are extended stored procedures used by the SQL Server Agent that provide privileged actions that run externally to the DBMS under the security context of the SQL Server Agent service account. If these procedures are available from a database session, an exploit to the SQL Server instance could result in a compromise of the host system and external SQL Server resources. Access to these procedures should be disabled unless use of SQL Server Agent is required and authorized.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'agent xps'
```

If the value of Config_Value is 1, confirm in the System Security Plan that this option is documented, required and approved by the IAO. If it is not documented, required and approved, this is a Finding.

Note: If you are using SQL Server Management Studio to administer the SQL Server DBMS, document, approve and enable this option in the System Security Plan.

Fix:

Authorize and document requirements for use of the Agent XPs option in the System Security Plan and AIS Functional Architecture documentation. Where not required and authorized, disable its use.

For SQL Server 2005:

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'Agent XPs', 0
RECONFIGURE
```

VKEY: V0015210	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

4.165 DM6199: SMO and DMO XPs option

Description: The SMO and DMO XPs are management object extended stored procedures that provide highly privileged actions that run externally to the DBMS under the security context of the SQL Server service account. If these procedures are available from a database session, an exploit to the SQL Server instance could result in a compromise of the host system and external SQL Server resources including the SQL Server software, audit, log and data files. Access to these procedures should be disabled unless a clear requirement for their use is indicated and authorized.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT CAST(value AS INT) 'Config_Value'
FROM [master].sys.configurations
WHERE name = 'smo and dmo xps'
```

If the value of Config_Value is 1, confirm in the System Security Plan and AIS Functional Architecture documentation that this option is documented and is required and approved by the IAO. If it is not documented, required and approved, this is a Finding.

Note: If you are using SQL Server Management Studio to administer the SQL Server DBMS, document, approve and enable this option in the System Security Plan.

Fix:

Authorize and document requirements for use of the SMO and DMO XPs option in the System Security Plan and AIS Functional Architecture documentation. Where not required and authorized, disable its use.

For SQL Server 2005:

From the query prompt:

```
EXEC SP_CONFIGURE 'show advanced options', 1
EXEC SP_CONFIGURE 'SMO and DMO XPs', 0
RECONFIGURE
```

VKEY: V0015211	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: False	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.1			
STIG Requirement:	(DG0099: CAT II) The DBA will disable use of external procedures by the database unless mission and/or operationally required and documented in the AIS functional architecture documentation.			

5. SQL Server Database Check Procedures

5.1 DG0004: DBMS application object owner accounts

Description: Object ownership provides all database object permissions to the owned object. Access to the application object owner accounts requires special protection to prevent unauthorized access and use of the object ownership privileges. In addition to the high privileges to application objects assigned to this account, it is also an account that, by definition, is not accessed interactively except for application installation and maintenance. This reduced access to the account means that unauthorized access to the account could go undetected. To help protect the account, it should be disabled only when access is required.

Check:

Review list of non-default, non-DBA and non-developer object owners:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT DISTINCT uid
FROM sysobjects
WHERE crdate > (SELECT DATEADD(day, 1, crdate)
 FROM [master].dbo.sysobjects
 WHERE name = 'syslogins')
```

For each object owner uid returned:

From the query prompt:

```
USE [database name]
SELECT s.name
FROM sysusers u, [master].dbo.syslogins s
WHERE u.sid = s.sid
AND u.uid = '[uid]'
AND (s.denylogin = 0 OR s.hasaccess = 1)
AND (u.issqlrole = 0 AND u.isapprole = 0)
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT DISTINCT schema_id
FROM sys.all_objects
WHERE is_ms_shipped = 0
```

For each schema_id returned:

From the query prompt:

```
SELECT DISTINCT SUSER_NAME(schema_id)
FROM sys.all_objects
WHERE is_ms_shipped = 0
```

If any login names are returned (not disabled) from the last part of the query, this is a Finding.

Note: The 'sa' account is not exempt from this requirement and should be disabled. DBA and developer accounts authorized to own objects in the database are exempt from this requirement.

Fix:

Disable logins for all application object owner accounts or members of database roles that own objects:

```
ALTER LOGIN [name] DISABLE
```

Document application object owner accounts in the System Security Plan.

VKEY: V0005683	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Auto	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.3			
STIG Requirement:	(DG0004: CAT II) The DBA will ensure custom application owner accounts are disabled or locked when not in use.			

5.2 DG0008: DBMS application object ownership

Description: SQL Server objects include tables, views, stored procedures, triggers, defaults and rules. The user that creates an object becomes the object owner. For security and performance reasons, only the database owner should be allowed to create and own objects. Checking for objects that were not created by the database owner helps ensure that Trojan horses and other unauthorized changes have not been made to the server. Having multiple object owners also degrades performance. SQL Server performs optimally when using ownership chains. An ownership chain exists when objects reference other objects that have the same owner. SQL Server bypasses the work of performing security checks on other objects in the chain.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT DISTINCT u.name
FROM sysusers u, sysobjects o
WHERE u.uid = o.uid
AND u.uid NOT IN ('1', '3', '4')
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT DISTINCT u.name
FROM sys.database_principals u, sys.all_objects o
```

```
WHERE u.principal_id = o.schema_id
AND u.principal_id NOT IN ('1', '3', '4')
```

Verify with the DBA that any accounts noted are authorized application installation accounts.

Objects that are owned by users "INFORMATION_SCHEMA" and "SYSTEM_FUNCTION_SCHEMA" are Not a Finding.

If any other accounts are not authorized, this is a Finding.

Fix:

Create database accounts dedicated for application object ownership. To simplify access authorizations, use a single account for each application to avoid cross chaining of ownership, which makes security configuration more complex and degrades system performance.

Document all authorized application object ownership in the System Security Plan.

VKEY: V0015607	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0008: CAT II) The DBA will ensure database application objects are owned by an authorized application object owner account.			

5.3 DG0015: DBMS data definition language use

Description: Application users by definition and job function require only the permissions to manipulate data within database objects and execute procedures within the database. The statements used to define objects in the database are referred to as Data Definition Language (DDL) statements and include the CREATE, DROP, and ALTER object statements. (DDL statements do not include CREATE USER, DROP USER or ALTER USER actions.) This requirement is included here, as a production system would not support changes to the data definitions. Where object creation is an indirect result of DBMS operation or dynamic object structures are required by the application function as is found in some object-oriented DBMS applications, this restriction does not apply. Re-use of static data structures to recreate temporary data objects are not exempted.

Check:

View a list of objects in the database. If any object creation dates do not coincide with the software maintenance and upgrade logs or are not objects documented as supporting dynamic object creation functions, investigate the circumstances under which the object was created. If the object is created using static definitions to store temporary data or indicates that the application uses unauthorized DDL statements, this is a Finding.

To view object creation dates created 1 day or later than the database installation:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT name, crdate
FROM sysobjects
WHERE crdate > (SELECT DATEADD(day, 1, crdate)
 FROM [master].dbo.sysobjects
 WHERE name = 'syslogins')
AND uid <> 1
ORDER BY name, crdate
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
AND state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT name, create_date
FROM sys.all_objects
WHERE is_ms_shipped = 0
AND schema_id <> 1
ORDER BY name, create_date
```

The results of these queries will just give an indication of what objects were created since the database installation or its most recent upgrade. It should not be used as a complete result. For example, application objects created with the database installation will not be reported.

To view objects created by an account that is not the DBO, INFORMATION_SCHEMA or system_function_schema:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT USER_NAME(uid), name, crdate
FROM sysobjects
WHERE uid NOT IN (1, 3, 4)
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
AND state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT USER_NAME(schema_id), name, create_date
FROM sys.all_objects
WHERE schema_id NOT IN (1, 3, 4)
```

These results will show objects created by a non-default user. If the creation dates are more recent than the installation or latest upgrade of the application, the application may use DDL statements.

Fix:

Coordinate with the application designer to modify the application to use static objects with temporary data rather than creating and using temporary objects.

Document in the System Security Plan all known object creation that supports dynamic object usage.

VKEY: V0003727	Severity: CAT 3		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECSD	Check Type: Verify	Database Level: True	Responsibility: IAO	Documentable: False
Reference:	Database STIG 3.3.20			
STIG Requirement:	(DG0015: CAT III) The IAO will ensure database applications do not use DDL statements except where dynamic object structures are required.			

5.4 DG0091: DBMS source code encoding or encryption

Description: Source code may include information on data relationships, locations of sensitive data that are otherwise obscured, or other processing information that could aid a malicious user. Encoding or encryption of the custom source code objects within the database helps protect against this type of disclosure.

Check:

If this is not a production database, this check is Not a Finding.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT o.name
FROM sysobjects o, syscomments c
WHERE o.id = c.id
AND o.uid NOT IN (1, 3, 4)
AND o.crdate > (SELECT DATEADD(day, 1, crdate)
 FROM [master].dbo.sysobjects
 WHERE name = 'syslogins')
AND c.encrypted = 0
AND o.type IN ('TR', 'X', 'P', 'FN', 'IF', 'RF')
AND o.category = 0
ORDER BY o.name
```

If any results are listed that are not installed as part of a COTS application, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
```

AND state = 0

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT o.name
FROM sys.all_objects o, sys.sql_modules s
WHERE o.object_id = s.object_id
AND s.definition IS NOT NULL
AND o.schema_id NOT IN (1, 3, 4)
ORDER BY o.name
```

If any results are listed that are not installed as part of a COTS application, this is a Finding.

Fix:

Recreate stored procedures and specify encryption in the CREATE PROCEDURE command.

Example:

```
CREATE OR REPLACE PROCEDURE [MyProc] WITH ENCRYPTION
AS
SELECT [mycol1], [mycol2] FROM [mytable]
```

Replace objects specified between the "[]" characters with custom/GOTS procedure references.

VKEY: V0003823	Severity: CAT 3		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCSL	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.10			
STIG Requirement:	(DG0091: CAT III) The DBA will ensure custom application and Government-Off-The-Shelf (GOTS) source code objects are encoded or encrypted within the production database where supported by the DBMS.			

5.5 DG0105: DBMS application user role privilege assignment

Description: Unauthorized access to the data can lead to loss of confidentiality and integrity of the data.

Check:

Compare privileges assigned to database application user roles to those defined in the System Security Plan.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

```
USE [database name]
SELECT u.name, o.name, p.action
FROM sysprotects p, sysusers u, sysobjects o
WHERE p.id = o.id
AND p.uid = u.uid
AND p.uid NOT IN (0, 2)
AND (u.issqlrole = 1 OR u.isapprole = 1)
AND p.protecttype IN (204, 205)
ORDER BY u.name, o.name, p.action
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
AND state = 0
```

Repeat for each database:

```
USE [database name]
SELECT r.name, o.name, p.permission_name
FROM sys.database_principals r, sys.database_permissions p, sys.all_objects o
WHERE p.grantee_principal_id = r.principal_id
AND p.major_id = o.object_id
```

```
AND r.principal_id NOT IN (0, 2)
AND r.type IN ('A', 'R')
AND r.is_fixed_role = 0
ORDER BY r.name, o.name, p.permission_name
```

If the assigned privileges do not match the authorized list of privileges, this is a Finding.

Note: Default privileges assigned to fixed data roles are considered authorized by default.

Fix:

Use the grant and revoke commands to assign the authorized privileges as listed in the System Security Plan to custom database application or application user roles.

VKEY: V0015128	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: DCFA	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.1.4.2			
STIG Requirement:	(DG0105: CAT II) The DBA will ensure all database application user roles and the privileges assigned to them are authorized by the Information Owner in the AIS functional architecture documentation.			

5.6 DG0121: DBMS application user privilege assignment

Description: Privileges granted outside the role of the application user job function are more likely to go unmanaged or without oversight for authorization. Maintenance of privileges using roles defined for discrete job functions offers improved oversight of application user privilege assignments and helps to protect against unauthorized privilege assignment.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name, o.name, p.action
FROM sysprotects p, sysobjects o, dbo.sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND p.protecttype IN (204, 205)
AND (u.issqluser = 1 or u.isntuser = 1)
ORDER BY u.name, o.name, p.action
```

Action Types returned in the query are:

26 - REFERENCES
193 - SELECT
195 - INSERT
197 - UPDATE
196 - DELETE
224 - EXECUTE

If any names are listed, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name
```

```
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name, o.name, p.permission_name
FROM sys.all_objects o, sys.database_principals u, sys.database_permissions
p
WHERE o.object_id = p.major_id
AND p.grantee_principal_id = u.principal_id
AND p.state IN ('G', 'W')
AND u.type IN ('S', 'U')
ORDER BY u.name, o.name, p.permission_name
```

If any names are listed, this is a Finding.

Fix:

Revoke permissions assigned directly to user accounts and grant them instead to the appropriate group account.

From the query prompt:

```
REVOKE [permission] ON [object] FROM [user name]
GRANT [permission] ON [object] TO [group name]
```

Document any exceptions to privileges that cannot be assigned via database roles in the System Security Plan.

VKEY: V0015629	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Auto	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0121: CAT II) The DBA will ensure database privileges are assigned via roles and not directly assigned to database accounts. Privileges may be assigned directly to application owner accounts where the DBMS does not otherwise support access via roles.			

5.7 DG0122: Sensitive data access

Description: Unauthorized access to sensitive data can lead to unauthorized disclosure, modification or accountability. Access to sensitive data that is granted that is not restricted at all levels based on job function may be exploited regardless of attempts to control. An example of this is a web application that serves general users, but that access sensitive data in a backend database using an account with elevated privileges. This provides a means for the web application user to exploit the application to gain unauthorized access to data in the database. Where the user never has access to a path with excess privileges, unauthorized access is more difficult to gain.

Check:

If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan and/or AIS Functional Architecture documentation, this check is Not a Finding.

Review privilege assignments to sensitive data stored in the database.

Compare assigned privileges to those that are authorized in the System Security Plan.

If unauthorized access is granted or sensitive data access requirements are not documented, this is a Finding.

Fix:

Have the Information Owner identify all sensitive data stored in the database specified in the System Security Plan.

Define job functions and sensitive data access requirements for the job functions and included them in the System Security Plan.

Assign only authorized users for job functions.

VKEY: V0015630	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECAN	Check Type: Manual	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0122: CAT II) The DBA will ensure all access to sensitive administrative DBMS data stored inside the database and in external host files is granted only to DBA and other authorized administrative database and OS accounts.			

5.8 DG0138: DBMS access to sensitive data

Description: Unauthorized access to sensitive data may compromise the confidentiality of personnel privacy, threaten national security or compromise a variety of other sensitive operations. Access controls are best managed by defining requirements based on distinct job functions and assigning access based on the job function assigned to the individual user.

Check:

If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan and/or AIS Functional Architecture documentation, this check is Not a Finding.

Review data access requirements for sensitive data as identified and assigned by the Information Owner in the System Security Plan.

Review the access controls for sensitive data configured in the database.

If the configured access controls do not match those defined in the System Security Plan, this is a Finding.

Fix:

Define, document and implement all sensitive data access controls based on job function in the System Security Plan.

VKEY: V0015642	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECAN	Check Type: Interview	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.1			
STIG Requirement:	(DG0138: CAT II) The DBA will ensure all access to sensitive application data stored or defined within database objects is granted only to database application user roles and not directly to database application user accounts.			

5.9 DG0165: DBMS symmetric key management

Description: Unauthorized access to the database master key could jeopardize the confidentiality of sensitive data stored in the database. Access to the database master key should be strictly assigned to a limited number of individuals authorized to use and maintain the key.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT USER_NAME(grantee_principal_id)
FROM sys.database_permissions
WHERE class = 0
AND state IN ('G', 'W')
AND type = 'CL'
ORDER BY USER_NAME(grantee_principal_id)
```

If no records are returned, this is Not a Finding.

If any records are returned, verify they are authorized to have access to manage the Database Master Key. If any do not, this is a Finding.

Fix:

Document all users authorized to access the database master key in the System Security Plan.

Restrict authorized users to the application, database owner and SYSADMINs.

For SQL Server 2005:

For each unauthorized user:

From the query prompt:

```
REVOKE CONTROL FROM [user name]
```

VKEY: V0015654	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3			
STIG Requirement:	(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.			

5.10 DG0166: Protection of DBMS asymmetric encryption keys

Description: Encryption is only effective if the encryption method is robust and the keys used to provide the encryption are not easily discovered. Without effective encryption, sensitive data is vulnerable to unauthorized access.

Check:

If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan and/or AIS Functional Architecture documentation, this check is Not a Finding.

Note: Protection of DBMS system data is reviewed in other checks.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT k.name, SUSER_SNAME(u.sid), k.pvt_key_encryption_type
FROM sys.asymmetric_keys k, sys.database_principals u
WHERE k.principal_id = u.principal_id
ORDER BY k.name, SUSER_SNAME(u.sid), k.pvt_key_encryption_type
```

If the total number of records returned for all databases is 0, this is Not a Finding.

Note: Compliance will be measured as part of the security review of the application.

For each asymmetric key identified as being used to encrypt sensitive date, verify the key owner is not a SYSADMIN:

From the query prompt:

```
USE [database name]
SELECT o.name, USER_NAME(p.grantee_principal_id), p.permission_name
FROM sys.database_permissions p, sys.objects o
WHERE p.major_id = o.object_id
AND p.class_desc = 'ASYMMETRIC KEY'
ORDER BY o.name, USER_NAME(p.grantee_principal_id),
p.permission_name
```

If the key owner listed from the previous query is listed as a sysadmin member, this is a Finding.

If any key owner of a key listed above is not the application object owner account or an account specific to the application as documented in the System Security Plan, this is a Finding.

Review any asymmetric keys whose private key is not encrypted:

From the query prompt:

```
SELECT name
FROM [master].sys.asymmetric_keys
WHERE pvt_key_encryption_type = 'NA'
ORDER BY name
```

If any records are returned, this is a Finding.

Examine evidence that an audit record is created whenever the asymmetric key is accessed by other than authorized users. In particular, view evidence that access by a SYSADMIN or other system privileged account results in the generation of an audit record. This is required because system privileges allow access to encryption keys and can use them to access sensitive data where they do not have a need to know.

If an audit record is not generated for unauthorized access to the asymmetric key, this is a Finding.

Note: SQL Server does not provide use of encryption keys stored outside of the instance except to create keys stored within the instance. Therefore, protection of externally stored keys is not addressed for SQL Server in this check.

Fix:

For SQL Server 2005:

Use DOD code-signing certificates to create asymmetric keys stored in the database and used to encrypt sensitive data stored in the database.

Assign the application object owner account as the owner of the asymmetric key.

Create audit events for access to the key by other than the application owner account or approved application objects.

Revoke any privileges assigned to the asymmetric key to other than the application object owner account and authorized users.

Protect the private key by encrypting it with the database or service master key.

VKEY: V0015142	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3			
STIG Requirement:	(DG0166: CAT II) The DBA will ensure asymmetric keys used for encryption of sensitive data used by or for the DBMS use DOD PKI certificates and will ensure the private keys are protected and stored in accordance with NIST (unclassified data protection) or NSA (classified data protection)-approved key management technology and processes.			

5.11 DG0172: DBMS classification level audit

Description: Some DBMS systems provide the feature to assign security labels to data elements. The confidentiality and integrity of the data depends upon the security label assignment where this feature is in use. Changes to security label assignment may indicate suspicious activity.

Check:

If no data is identified as being sensitive or classified by the Information Owner, in the System Security Plan or in the AIS Functional Architecture documentation, this check is Not a Finding.

If no identified sensitive or classified data requires encryption by the Information Owner in the System Security Plan and/or AIS Functional Architecture documentation, this check is Not a Finding.

If the DBMS does not provide the capability to display sensitivity marking of data, this check is Not a Finding.

For SQL Server 2005:

Review the DBMS configuration for marking and labeling of sensitive data.

http://www.microsoft.com/technet/prodtechnol/sql/2005/multisec.mspx

If security label assignment is not audited for changes, this is a Finding.

Fix:

For SQL Server 2005:

Define the policy for auditing changes to security labels defined for the data. Document the audit requirements in the System Security Plan and configure database auditing in accordance with the policy.

VKEY: V0015657	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CS;2-CS;3-CS
IA Control: ECLC	Check Type: Manual	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.9			
STIG Requirement:	(DG0172: CAT II) The DBA will enable auditing of any changes to the classification or sensitivity level assigned to classified data in the DBMS where available and required by the Information Owner.			

5.12 DM0531: Fixed database role members

Description: Fixed database roles provide a mechanism to grant groups of privileges to users. These privilege groupings are defined by the installation or upgrade of the SQL Server software at the discretion of Microsoft. Memberships in these roles granted to users should be strictly controlled and monitored. Privileges assigned to these roles should be reviewed for change after software upgrade or maintenance to ensure that the privileges continue to be appropriate to the assigned members.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', g.name 'Group'
FROM sysmembers s, sysusers u, sysusers g
WHERE s.memberuid = u.uid
AND s.groupuid = g.uid
AND g.name IN ('db_owner', 'db_accessadmin', 'db_datareader',
'db_datawriter', 'db_ddladmin', 'db_securityadmin', 'db_backupoperator',
'db_denydatareader', 'db_denydatawriter')
ORDER BY u.name, g.name
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', g.name 'Group'
```

```
FROM sys.database_role_members r, sys.database_principals u,
sys.database_principals g
WHERE r.role_principal_id = g.principal_id
AND r.member_principal_id = u.principal_id
AND g.is_fixed_role = 1
ORDER BY u.name, g.name
```

The DBO membership in the db_owner fixed database role does not require explicit authorization and is Not a Finding.

Verify authorization of each member listed in the System Security Plan. If any members are not authorized, this is a Finding.

Fix:

Grant fixed roles to authorized personnel only. Remove unauthorized accounts from assigned roles.

For SQL Server 7 & 2000:

From the SQL Server Enterprise Manager GUI:

To deassign roles:

1. Expand [instance name]
2. Expand Databases
3. Expand [database type]
4. Expand [database name]
5. Expand Security
6. Expand Roles
7. Expand Database Roles
8. Double-click the role to be removed from the assigned user
9. Select the user's account under Role Members
10. Click on the Remove button

For SQL Server 2005:

From the SQL Server Management Studio GUI:

To deassign roles:

1. Expand [instance name]
2. Expand Databases
3. Expand [database type]
4. Expand [database name]
5. Expand Security
6. Expand Roles
7. Expand Database Roles
8. Double-click the role to be removed from the assigned user

9. Select the user's account under Role Members
10. Click on the Remove button

VKEY: V0015151	Severity: CAT 2		Policy: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Manual	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0119: CAT II) The DBA will ensure database application user roles are restricted to select, insert, update, delete, and execute privileges.			

5.13 DM1709: Guest user

Description: The guest user ID in a database allows access by all Windows login IDs without requiring an individual database account. This allows unauthorized access to the database.

Check:

For SQL Server 7 & 2000:

Note: The guest account cannot be removed from the master or tempdb database in SQL Server 2000.

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE name NOT IN ('master', 'tempdb')
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT COUNT(uid)
FROM sysusers
WHERE uid = 2
AND hasdbaccess = 1
```

If any value other than a 0 is returned, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE name NOT IN ('master', 'tempdb')
AND state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT COUNT(grantee_principal_id)
```

```
FROM sys.database_permissions
WHERE grantee_principal_id = 2
AND state = 'G'
AND permission_name = 'CONNECT'
```

If any value other than a 0 is returned, this is a Finding.

Fix:

For SQL Server 7, drop the Guest user account.

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE name NOT IN ('master', 'tempdb')
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
EXEC SP_DROPUSER 'guest'
```

For SQL Server 2000, revoke access to all databases except master and tempdb.

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE name NOT IN ('master', 'tempdb')
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
EXEC SP_REVOKEDBACCESS 'guest'
```

For SQL Server 2005, revoke connect permission from all databases except master and tempdb.

From the query prompt:

```
SELECT name
```

```
FROM [master].sys.databases
WHERE name NOT IN ('master', 'tempdb')
AND state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
REVOKE CONNECT FROM 'guest'
```

VKEY: V0002451	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAAC	Check Type: Auto	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.24			
STIG Requirement:	(DG0074: CAT II) The DBA will monitor database account expiration and inactivity and remove expired accounts and accounts that have been inactive for 35 days or longer or the site maximum limit.			

5.14 DM1715: Unauthorized object permission grants

Description: Securely designed applications require only that database application user accounts have permissions to access and manipulate only the application data assigned to them in accordance with the their job function. Restrictions may be further restricted by granting data access to users only through execution of database procedures. Excess privileges can lead to unauthorized data access and can compromise data integrity.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE name NOT IN ('master', 'tempdb')
AND DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object', p.action 'Action'
FROM sysprotects p, sysobjects o, sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND p.protecttype IN (204, 205)
AND (p.action NOT IN (193, 195, 196, 197, 224) OR p.uid IN (0, 2))
ORDER BY u.name, o.name, p.action
```

Action Types returned in the query are:

26 - REFERENCES
193 - SELECT
195 - INSERT
197 - UPDATE
196 - DELETE
224 - EXECUTE

If any results are reported for Public or Guest, this is a Finding.

If any results are for system objects, this is a Finding.

Note: Some permissions assigned to PUBLIC within the master database may require that the 'Allow modifications to be made directly to the system catalogs' database setting be temporarily be enabled.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE name NOT IN ('tempdb', 'ReportServerTempDB')
AND state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object', p.permission_name 'Action'
FROM sys.all_objects o, sys.database_principals u, sys.database_permissions
p
WHERE o.object_id = p.major_id
AND p.grantee_principal_id = u.principal_id
AND p.state IN ('G', 'W')
AND (p.type NOT IN ('DL', 'EX', 'IN', 'SL', 'UP')
 OR u.name IN ('public', 'guest'))
ORDER BY u.name, o.name, p.permission_name
```

If any names are listed, this is a Finding.

Fix:

Revoke unauthorized permissions assigned to application user roles.

From the query prompt:

```
USE [database name]
REVOKE [permission] ON [object] FROM [group name]
```

VKEY: V0002457	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0119: CAT II) The DBA will ensure database application user roles are restricted to select, insert, update, delete, and execute privileges.			

5.15 DM1749: System table permissions

Description: Microsoft SQL Server defaults to allow all users to view the majority of the system tables. The system tables contain information such as login IDs, permissions, objects and even the text of all stored procedures. In a secure environment, any direct access granted to these tables by users bypasses security controls defined within the associated system procedures and views. The bypass of these controls can lead to unauthorized viewing of sensitive data.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name, o.name, p.action
FROM sysprotects p, sysobjects o, sysusers u
WHERE o.id = p.id
AND p.uid = u.uid
AND p.protecttype IN (204, 205)
AND o.type = 'S'
ORDER BY u.name, o.name, p.action
```

Action Types returned in the query are:

26 - REFERENCES
193 - SELECT
195 - INSERT
197 - UPDATE
196 - DELETE
224 - EXECUTE

If results are listed for any database, this is a Finding.

Note: By default, public select permission is granted to system tables in all databases. Even though permission is set by default, it is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object', p.permission_name 'Action'
FROM sys.all_objects o, sys.database_principals u, sys.database_permissions
p
WHERE o.object_id = p.major_id
AND p.grantee_principal_id = u.principal_id
AND p.state in ('G','W')
AND (p.type LIKE 'CR%' OR p.type LIKE 'AL%')
ORDER BY u.name, o.name, p.permission_name
```

If results are listed for any database, this is a Finding.

Note: By default, public select permission is granted to system tables in all databases. Even though permission is set by default, it is a Finding.

Fix:

Revoke permissions granted to system tables.

For each listed from the check query:

From the query prompt:

```
USE [database name]
REVOKE [permission] ON [object name] FROM [user name]
```

VKEY: V0002458	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Auto	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0080: CAT II) The DBA will ensure privileges granted to application user database accounts are restricted to those required to perform the specific application functions.			

5.16 DM1760: DDL permission assignments

Description: Data Definition Language (DDL) commands include CREATE, ALTER, and DROP object actions. These actions cause changes to the structure, definition and configuration of the DBMS as well as to the objects themselves that can affect any or all operations of the database. Such privileged actions, when not restricted to authorized persons and activities, can lead to a compromise of data and DBMS availability.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object', p.action 'Action'
FROM sysprotects p, sysobjects o, sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND p.protecttype IN (204, 205)
AND p.action NOT IN (193, 195, 196, 197, 224)
ORDER BY u.name, o.name, p.action
```

Action Types returned in the query are:

```
26 - REFERENCES
178 - CREATE FUNCTION
198 - CREATE TABLE
203 - CREATE DATABASE
207 - CREATE VIEW
222 - CREATE PROCEDURE
228 - BACKUP DATABASE
233 - CREATE DEFAULT
235 - BACKUP LOG
236 - CREATE RULE
```

The numbers returned correspond to the Action types listed above.

Compare the results to the System Security Plan. If any accounts listed are application users, application user roles, or application administrator roles, public or guest, this is a Finding.

If any application developer accounts are listed with DDL privileges to production databases, this is a Finding.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object', p.permission_name 'Action'
FROM sys.database_permissions p, sys.database_principals u, sys.all_objects
o
WHERE o.object_id = p.major_id
AND p.grantee_principal_id = u.principal_id
AND p.state IN ('G', 'W')
AND (p.type LIKE 'CR%' OR p.type LIKE 'AL%')
ORDER BY u.name, o.name, p.permission_name
```

Compare the results to the System Security Plan. If any accounts listed are application users, application user roles, or application administrator roles, public or guest, this is a Finding.

If any application developer accounts are listed with DDL privileges to production databases, this is a Finding.

Fix:

Revoke DDL privileges from unauthorized accounts with the REVOKE command:

From the query prompt:

```
USE [database name]
REVOKE [permission] FROM [user name]
```

VKEY: V0002463	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0119: CAT II) The DBA will ensure database application user roles are restricted to select, insert, update, delete, and execute privileges.			

5.17 DM5144: WITH GRANT privilege assignments

Description: The WITH GRANT option assigned with privileges, allows the grantee of the privilege to re-grant the privilege to other accounts. Unauthorized or unmanaged assignment of privileges may result in a compromise of data confidentiality and database operation. Privilege assignment should be restricted to DBA, application object owner accounts and application administration accounts.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object', p.action 'Action'
FROM sysprotects p, sysobjects o, sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND p.protecttype = 204
ORDER BY u.name, o.name, p.action
```

Action Types returned in the query are:

26 - REFERENCES
193 - SELECT
195 - INSERT
197 - UPDATE
196 - DELETE
224 - EXECUTE

For all listed objects, validate with the DBA permissions granted with the Grant Option are assigned to application administrator roles only. If any are not, this is a Finding.

For SQL Server 2005:

From the query prompt:

SELECT name
FROM [master].sys.databases
WHERE state = 0

Repeat for each database:

From the query prompt:

USE [database name]
SELECT u.name 'User', o.name 'Object', p.permission_name 'Action'
FROM sys.database_permissions p, sys.database_principals u, sys.all_objects o
WHERE o.object_id = p.major_id
AND p.grantee_principal_id = u.principal_id
AND p.state = 'W'
ORDER BY u.name, o.name, p.permission_name

For all listed objects, validate with the DBA permissions granted with the Grant Option are assigned to application administrator roles only. If any are not, this is a Finding.

Fix:

Revoke unauthorized privileges granted with the WITH GRANT option.

From the query prompt:

USE [database name]
REVOKE GRANT OPTION FOR [object name] FROM [user name]

VKEY: V0002498	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0119: CAT II) The DBA will ensure database application user roles are restricted to select, insert, update, delete, and execute privileges.			

5.18 DM6175: Database Master key encryption password

Description: Weak passwords may be easily guessed. When passwords used to encrypt keys used for encryption of sensitive data, then the confidentiality of all data encrypted using that key is at risk.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT COUNT(name)
FROM sys.symmetric_keys s, sys.key_encryptions k
WHERE s.name = '##MS_DatabaseMasterKey##'
AND s.symmetric_key_id = k.key_id
AND k.crypt_type = 'ESKP'
```

If the value returned is greater than 0, a Database Master key exists and is encrypted with a password.

Review procedures and evidence of password requirements used to encrypt Database Master Keys. If the passwords are not required to meet DOD password standards, currently 15 characters, 2 uppercase characters, 2 lowercase characters, 2 special characters, and 2 numeric characters and no repeating characters, this is a Finding.

Interview the IAO or DBA to determine the method to retrieve the password to use the Database Master Key. If storage of the password occurs unencrypted in application code or other database tables or files, this is a Finding.

Fix:

For SQL Server 2005:

Assign an encryption password to the Database Master Key that is a minimum of 15 characters, contains at least 2 uppercase characters, 2 lowercase characters, 2 special characters, 2 numeric characters and has no repeating characters.

To change the Database Master Key encryption password:

```
USE [database name]
ALTER MASTER KEY REGENERATE WITH ENCRYPTION BY
PASSWORD = '[new password]'
```

Note: The database master key encryption method should not be changed until the effects are thoroughly reviewed. Changing the master key encryption causes all encryption using the database master key to be decrypted and re-encrypted. This action should not be taken during a high-demand time. Please see the MS SQL Server documentation prior to re-encrypting the database master key for detailed information.

VKEY: V0015159	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3			
STIG Requirement:	(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.			

5.19 DM6179: Database Master key encrypted by server

Description: Protection of the Database Master Key is necessary to protect the confidentiality of sensitive data. When encrypted by the Service Master Key, SYSADMINs may access and use the key to view sensitive data that they are not authorized to view. Where alternate encryption means are not feasible, encryption by the Service Master Key may be necessary. To help protect sensitive data from unauthorized access by DBA's, mitigations may be in order. Mitigations may include automatic alerts or other audit events when the database master key is accessed outside of the application or by a DBA account.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE is_master_key_encrypted_by_server = 1
AND owner_sid <> 1
AND state = 0
```

If no databases are returned, this is Not a Finding.

For any databases returned, verify in the System Security Plan that encryption of the Database Master Key using the Service Master Key is acceptable and approved by the Information Owner and the encrypted data does not require additional protections to deter or detect DBA access. If not approved, this is a Finding.

If approved and additional protections are required, then verify that the additional requirements are in place in accordance with the System Security Plan. These may include additional auditing on access of the Database Master Key with alerts or other automated monitoring.

If the additional requirements are not in place, this is a Finding.

Fix:

For SQL Server 2005:

Where possible, encrypt the Database Master Key with a password known only to the application administrator.

Where not possible, configure additional audit events or alerts to detect unauthorized access to the database master key by users not authorized to view sensitive data.

VKEY: V0015161	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3			
STIG Requirement:	(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.			

5.20 DM6180: Database Master key password storage

Description: Storage of the database master key password in a database credential allows decryption of sensitive data by privileged users who may not have a need-to-know requirement to access the data.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT COUNT(credential_id)
FROM [master].sys.master_key_passwords
```

If count is not 0, this is a Finding.

Fix:

Use the stored procedure sp_control_dbmasterkey_password to remove any credentials that store database master key passwords.

For SQL Server 2005:

From the query prompt:

```
EXEC SP_CONTROL_DBMASTERKEY_PASSWORD @db_name =
'[database name]', @action = N'drop'
```

VKEY: V0015162	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Auto	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3			
STIG Requirement:	(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.			

5.21 DM6183: Symmetric keys encrypting mechanism

Description: Symmetric keys are vulnerable if the symmetric key encryption is not protected from disclosure. Symmetric keys are well protected by use of either the database or the service master key. Where access by DBA's is not acceptable, use of the application code-signing certificate can be used to provide protection.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT s.name, k.crypt_type_desc
FROM sys.symmetric_keys s, sys.key_encryptions k
WHERE s.symmetric_key_id = k.key_id
AND k.crypt_type IN ('KSKP', 'ESKS')
AND s.principal_id <> 1
ORDER BY s.name, k.crypt_type_desc
```

Review any symmetric keys that have been defined against the System Security Plan.

If any keys are defined that are not documented in the System Security Plan, this is a Finding.

Review the System Security Plan to review the encryption mechanism specified for each symmetric key. If the method does not indicate use of certificates, this is a Finding.

If the certificate specified is not a DOD PKI certificate, this is a Finding.

Fix:

For SQL Server 2005:

Configure or alter symmetric keys to encrypt keys with certificates or authorized asymmetric keys:

From the query prompt:

ALTER SYMMETRIC KEY [key name] ADD ENCRYPTION BY CERTIFICATE [certificate name]
ALTER SYMMETRIC KEY [key name] DROP ENCRYPTION BY [password, symmetric key or asymmetric key]

The symmetric key must specify a certificate or asymmetric key for encryption.

The certificate may be the code-signing certificate used by the application.

VKEY: V0015168	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3			
STIG Requirement:	(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.			

5.22 DM6184: Asymmetric keys specify DOD PKI

Description: Asymmetric keys derived from self-signed certificates or self-generated by other means do not meet the security requirements of DOD that require validation by DOD trusted certificate authorities.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT name, SUSER_SNAME(sid)
FROM sys.asymmetric_keys
ORDER BY name, SUSER_SNAME(sid)
```

If no keys are defined for any database, this check is Not a Finding.

If keys are returned, verify the key is associated with a DOD PKI Certificate.

Evidence may include review of the certificate of a signed file used to read the key into the database.

If the key is not from a DOD PKI certificate or evidence cannot be determined or presented, this is a Finding.

Fix:

For SQL Server 2005:

Where asymmetric key use is required, the asymmetric should be generated using a code-signing certificate or using the database master key to encrypt the private key. Use of the asymmetric key is expected in DOD installations to be used to support symmetric keys that are in turn used to encrypt sensitive data.

In a DOD environment, asymmetric keys generated and stored within the SQL Server database are not expected to be used for storage of DOD PKI certificates associated with DOD personnel and used to authenticate them for any database access.

CREATE ASYMMETRIC KEY [key name]

OR

CREATE ASYMMETRIC KEY [key name] FROM [asymmetric key source]

[asymmetric key source] may be FILE = [strong file name] or EXECUTABLE FILE = 'executable file' or ASSEMBLY [assembly name]

Each of the asymmetric key sources is expected in a DOD environment to files signed with code-signing certificates issued by the DOD PKMO. Use of the database master key to encrypt is acceptable, especially where the key is generated using the service master key which in turn is generated from the server certificate. In cases where the DBAs are not trusted, use of external key sources is required.

VKEY: V0015164	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3			
STIG Requirement:	(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.			

5.23 DM6185: Asymmetric keys private key encryption type

Description: Asymmetric keys stored in the database that also include storage of the private key require protection from any unauthorized user. To protect unauthorized access and use of any asymmetric key by DBA's or users with SYSADMIN privileges, a password must be used to encrypt the private key. Use of the Database Master Key or Service Master Key allows access by the DBA. Consider the protection requirements for asymmetric key usage and document this in the System Security Plan. Avoid storage of static asymmetric private keys that is keys not generated and maintained for temporary session or other temporary usage, in the database.

Check:

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT name, pvt_key_encryption_type_desc
FROM sys.asymmetric_keys
WHERE pvt_key_encryption_type = 'PW'
ORDER BY name, pvt_key_encryption_type_desc
```

If no records are returned, this is Not a Finding.

Review any records returned and the encryption type listed. If any do not match the documented approved encryption method as specified in the System Security Plan, this is a Finding.

Fix:

For SQL Server 2005:

If stored with a private key, the private key is always encrypted either by a specified password, or by the database or service master key.

Create or alter the asymmetric key with the approved encryption type specified in the System Security Plan.

Document the approved encryption method after considering whether the DBA should be trusted to access the asymmetric key.

VKEY: V0015185	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Verify	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3			
STIG Requirement:	(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.			

5.24 DM6188: Service Master Key backup and offline storage

Description: Backup and recovery of the Service Master Key may be critical to the complete recovery of the database.

Check:

For SQL Server 2005:

Review procedures for and evidence of backup of the SQL Server Service Master Key in the System Security Plan.

If the procedures or evidence does not exist, this is a Finding.

If the procedures do not indicate offline and off-site storage of the Service Master Key, this is a Finding.

If procedures do not indicate access restrictions to the Service Master Key backup, this is a Finding.

Fix:

For SQL Server 2005:

Document and implement procedures to safely backup and store the service master key.

Include in the procedures methods to establish evidence of backup and storage and careful, restricted access and restoration of the service master key.

Also, include provisions to store the key offsite.

VKEY: V0015177	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: IAKM	Check Type: Interview	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.2.3`			
STIG Requirement:	(DG0165: CAT II) The DBA will ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.			

5.25 DM6196: DBMS object permission grants to PUBLIC or Guest

Description: The guest account is available to users that do not have authorized accounts on the database. The PUBLIC role is granted to all users of the database regardless of assigned job function. Assignment of object privileges to unauthorized users can compromise data integrity and/or confidentiality.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object, p.action 'Action'
FROM sysprotects p, sysobjects o, sysusers u
WHERE p.id = o.id
AND p.uid = u.uid
AND p.protecttype IN (204, 205)
AND p.uid IN (0, 2)
ORDER BY u.name, o.name, p.action
```

Action type descriptions:

26 – REFERENCES
193 – SELECT
196 – DELETE
197 – UPDATE
224 – EXECUTE

If any results are reported, this is a Finding.

Note: Some permissions assigned to PUBLIC within the master database may require that the 'Allow modifications to be made directly to the system catalogs' database setting be temporarily be enabled.

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name 'User', o.name 'Object', p.permission_name 'Action'
FROM sys.database_permissions p, sys.database_principals u, sys.all_objects
o
WHERE o.object_id = p.major_id
AND p.grantee_principal_id = u.principal_id
AND p.grantee_principal_id IN (0, 2)
ORDER BY u.name, o.name, p.permission_name
```

If any results are reported, this is a Finding.

Note: Some permissions assigned to PUBLIC within the master database may require that the 'Allow modifications to be made directly to the system catalogs' database setting be temporarily be enabled.

Fix:

Revoke any object privileges assigned to PUBLIC or GUEST.

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

For SQL Server 2005:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
WHERE state = 0
```

Repeat for each database:

From the query prompt:

USE [database name]
REVOKE [privilege] ON [object name] FROM '[public or guest]'

Repeat for each object privilege assigned to public or guest:

From the query prompt:

USE [database name]
REVOKE [permission] ON [schema name].[object name] TO PUBLIC

To determine correct schema name for the object, use:

For SQL Server 7 & 2000:

SELECT uid
FROM [master].dbo.sysobjects
WHERE name = '[object name]'

For SQL Server 2005:

SELECT SCHEMA_NAME(schema_id)
FROM [master].sys.all_objects
WHERE name = '[object name]'

VKEY: V0015172	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Auto	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0080: CAT II) The DBA will ensure privileges granted to application user database accounts are restricted to those required to perform the specific application functions.			

5.26 DM6197: Fixed server and database role assignments to Guest

Description: The guest account is the account used by unauthenticated users of the database. Assignment of privileges to the guest account is an assignment of privileges to an unauthorized account. Any access by unauthenticated and unauthorized users can lead to a compromise of the database operational integrity as well as data integrity and confidentiality.

Check:

For SQL Server 7 & 2000:

From the query prompt:

```
SELECT name
FROM [master].dbo.sysdatabases
WHERE DATABASEPROPERTYEX(name, 'Status') = 'ONLINE'
```

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name
FROM sysmembers s, sysusers u
WHERE s.groupuid = u.uid
AND s.memberuid = 2
```

If any rows are returned, this is a Finding.

For SQL Server 2005:

Find any server roles assigned to Guest:

From the query prompt:

```
SELECT u.name
FROM [master].sys.server_role_members s, [master].sys.server_principals u
WHERE s.role_principal_id = u.principal_id
AND s.member_principal_id = 2
```

Find any database roles assigned to Guest:

From the query prompt:

```
SELECT name
FROM [master].sys.databases
```

WHERE state = 0

Repeat for each database:

From the query prompt:

```
USE [database name]
SELECT u.name
FROM sys.database_role_members s, sys.database_principals u
WHERE s.role_principal_id = u.principal_id
AND s.member_principal_id = 2
```

If any rows are returned, this is a Finding.

Fix:

Revoke server and database roles assigned to Guest.

Repeat for each database role assigned:

From the query prompt:

```
USE [database name]
EXEC SP_DROPROLEMEMBER '[role name]'  'Guest'
```

For each server roles assigned:

From the query prompt:

```
USE master
EXEC SP_DROPSRVROLEMEMBER 'Guest'  '[server role name]'
```

VKEY: V0015171	Severity: CAT 2		Policies: All Policies	MAC/CONF: 1-CSP;2-CSP;3-CSP
IA Control: ECLP	Check Type: Auto	Database Level: True	Responsibility: DBA	Documentable: False
Reference:	Database STIG 3.3.11.1			
STIG Requirement:	(DG0119: CAT II) The DBA will ensure database application user roles are restricted to select, insert, update, delete, and execute privileges.			

6. Appendix A – IAVM Bulletin Compliance

As of this date, IAVM compliance for SQL Server-related notices is maintained in the Windows host STIGs. Please refer to the Windows STIG for IAVM compliance information on SQL Server products.

7. Appendix B – Record of Changes

Changes for June 2009:

This is a new checklist and incorporates all current SQL Server versions (SQL Server version 7, SQL Server 2000 and SQL Server 2005). SQL Server 2008 checks will be derived directly from VMS and provided in a separate checklist. Text for all checks was reviewed and updated to meet current STIG requirements.

Following is a list of checks that were added or removed from the previous releases:

Removed	Why	Added	Why
DG0018	Not in STIG	DG0001	Consolidated with DM0590
DG0053	Not Applicable to SQL Server	DG0003	Consolidated with DM1769
DM0500	Consolidated with DG0116	DG0004	Consolidated with DM0630
DM0590	Consolidated with DG0001	DG0008	Consolidated with DM1759
DM0630	Consolidated with DG0004	DG0009	Consolidated with DM3769
DM0710	Current SPs contain fix	DG0014	Consolidated with DM0923
DM0922	Consolidated with DG0124	DG0016	Check not previously covered
DM0923	Consolidated with DG0014	DG0025	Consolidated with DM6181
DM0925	Consolidated with DG0101	DG0029	Consolidated with DM5268
DM1459	Consolidated with DG0128	DG0051	Consolidated with DM6190
DM1703	Consolidated with DG0141	DG0052	Consolidated with DM6192
DM1714	Consolidated with DG0121	DG0084	Consolidated with DM6162
DM1759	Consolidated with DG0008	DG0090	Check not previously covered
DM1762	Consolidated with DG0099	DG0091	Consolidated with DM1803
DM1769	Consolidated with DG0003	DG0098	Check not previously covered
DM1803	Consolidated with DG0091	DG0099	Consolidated with DM1762
DM2133	Consolidated with DG0100	DG0100	Consolidated with DM2133
DM2143	Consolidated with DG0190	DG0101	Consolidated with DM0925
DM3769	Consolidated with DG0009	DG0115	Check not previously covered
DM5145	Current SPs contain fix	DG0116	Consolidated with DM0500
DM5268	Consolidated with DG0029	DG0117	Check not previously covered
DM5408	Current SPs contain fix	DG0119	Check not previously covered
DM5432	Consolidated with DG0145	DG0121	Consolidated with DM1714
DM6010	Consolidated with DG0131	DG0122	Check not previously covered
DM6124	Consolidated with DG0157	DG0123	Check not previously covered
DM6125	Consolidated with DM0900	DG0124	Consolidated with DM0922
DM6161	Consolidated with DM1758	DG0128	Consolidated with DM1459
DM6162	Consolidated with DG0084	DG0131	Consolidated with DM6010
DM6172	Consolidated with DG0151	DG0140	Check not previously covered
DM6177	Consolidated with DG0165	DG0141	Consolidated with DM1703
DM6181	Consolidated with DG0025	DG0142	Consolidated with DM6200
DM6190	Consolidated with DG0051	DG0145	Consolidated with DM5432

DM6192	Consolidated with DG0052	DG0151	Consolidated with DM6172
DM6200	Consolidated with DG0142	DG0155	Check not previously covered
		DG0157	Consolidated with DM6124
		DG0165	Consolidated with DM6177
		DG0190	Consolidated with DM2143

Many checks that were removed were consolidated under other checks.

Following is a list of some of the checks that were modified from the previous releases:

STIG ID	TITLE	CHANGE
DG0002	DBMS version upgrade plan	SQL code
DG0003	DBMS security patch level	SQL code, updated service pack and product version levels as of 1 May 2009
DG0014	DBMS demonstration and sample databases	SQL code, Added DataEncryptDemo to list
DG0025	DBMS encryption compliance	SQL code, revised check wording
DG0029	Database auditing	SQL code, revised check wording
DG0032	DBMS audit record access	SQL code
DG0051	Database job/batch queue monitoring	SQL code
DG0052	DBMS software access audit	Revised check/fix wording
DG0060	DBMS shared account authorization	SQL code
DG0063	DBMS Restore Permission	SQL code
DG0070	DBMS user account authorization	SQL code
DG0074	DBMS inactive accounts	SQL code
DG0109	DBMS dedicated host	Revised check/fix wording
DG0110	DBMS host shared with a security service	Revised check/fix wording
DG0114	Critical DBMS files fault protection	Revised check/fix wording

8. Appendix C – VMS SRR Process Guide for SQL Server

8.1 VMS Terminology

The following is a list of VMS terms and how they are used within these instructions.

Asset – This is the host system for the DBMS being reviewed. It is typically defined using the domain\computername, the IP address and/or the MAC address.

Installation Posture – This is the SQL Server Installation as defined in VMS for the SQL Server Instance under review. It is defined as a VMS posture on the host asset.

- A SQL Server instance is identified by the SQL Server Instance name.

Database Posture – This database as defined in VMS exists within the SQL Server Instance under review. It is defined as a VMS posture on the host asset.

- A database posture is identified by the SQL Server Database Name. Each SQL Server database has the default databases: master, msdb, tempdb and model. It is also expected that at least one custom application database is defined for each SQL Server instance. VMS requires that each database posture include a reference to a SQL Server Instance. A SQL Server installation posture must be defined prior to the creation of a database posture.

Target – The word "target" is used within the SRR script XML import file to designate a specific installation or database posture assigned to an asset defined in VMS. Compliance or "Finding" results included in the XML import file update the status of the security item within VMS for the "target" database/installation posture. SQL Server installation "targets" must include the SQL Server instance name to update correctly the vulnerability statuses of the instance under review. Database "targets" must include the both the installation posture (SQL Server instance name) as well as the database name to update correctly the vulnerability status for the database under review.

Element – The word "element" is used within a VMS XML import file to create an installation or database posture for the asset specified in the same import file. The SQL Server installation element must include the SQL Server instance name. The SQL Server database element must include the database name and reference the SQL Server instance name.

Vulnerability – The word "vulnerability" is an item of security significance in VMS. Vulnerabilities are assigned directly to assets or to the asset's postures. DBMS vulnerabilities are assigned to installation and database postures defined for an asset.

Identifier – The identifier is a name assigned to the database posture. For SQL Server installations (instances), the identifier is or must be the SQL Server instance name. For SQL Server databases, the identifier is or must be the SQL Server database name.

Parent Identifier – In the case of DBMS postures/targets, a parent identifier exists only for databases. The parent identifier is the SQL Server instance name where the database is defined. This indicates a "dependent relationship" of the database to the instance.

8.2 Database VMS Maintenance

Identify the VMS DBMS Host Asset and DBMS postures

Each DBMS to be tracked within VMS requires assignment to a host asset. The host asset is identified by name, IP address and MAC address. The SQL Server SRR script will prompt for the host asset identification data. If the asset data is incorrectly supplied to the script, the resulting XML import file will not be able to load the results.

The host asset and database postures may be created before importing results by importing the **VMSasset.xml** file. This file is created by the SQL Server SRR script. Creating the VMS database postures is the sole purpose for the VMSasset.xml file.

Note: The asset information should always be verified before importing either of the SRR XML results files to avoid the unintentional creation and/or finding results assignment to the wrong asset or database posture.

As mentioned above under VMS terminology, each DBMS defined within VMS requires a minimum of two posture definitions. These postures are the SQL Server Installation and SQL Server Database postures. Two postures are necessary to provide the level of granularity required for tracking each occurrence of vulnerability. For example, vulnerabilities defined at the instance level (e.g., authentication mode) occur only once per instance. Vulnerabilities defined at the database level (e.g., fixed database role membership) occur once per defined database.

VMS requires that an identifier be defined for each of the DBMS postures. If you are manually creating database postures, make sure that you assign the SQL Server instance name as the SQL Server Installation identifier. This allows for proper assignment of SRR script evaluation results from the resulting VMSimport.xml file.

If you are manually creating SQL Server database postures, specify the correct database name as defined within the SQL Server instance as the database identifier. This allows for proper assignment of SRR script evaluation results from the resulting VMSimport.xml file. Database postures must also include the SQL Server instance name as the "parent identifier" to identify correctly the database as belonging to a specific SQL Server instance.

To view/confirm the DBMS host asset and confirm/create DBMS postures:

1. Collect from the database host system, the following information:
   - The PRIMARY IP and MAC addresses defined for the host (ipconfig /all for Windows)
   - The host name (DOS environment variable %computername%)

2. In VMS, select the host asset supporting the DBMS
   - For System Administrators
     - From the left navigation frame on VMS 6, expand Asset Finding Maint[enance]
     - From the expanded list, select Assets / Findings
     - Under Navigation on the Asset and Finding Maintenance screen, expand By Location, expand the location where the asset resides, expand Computing, and select the asset where SQL Server is installed

   - For Reviewers
     - From the left navigation frame on VMS 6, expand Asset Finding Maint[enance]
     - From the expanded list, select Assets / Findings
     - Under Navigation on the Asset and Finding Maintenance screen, expand Visit, expand the location where the asset resides, expand Computing, and select the asset where SQL Server is installed

3. Verify the host name (under the General tab) matches the data collected
4. Verify the IP Address (under the Asset Identification tab) matches the data collected
5. Verify the MAC Address (under the Asset Identification tab) matches the data collected
6. Select the Asset Posture tab
7. Under Selected, expand the asset name, expand Application, expand Database, expand SQL Server, expand or select SQL Server Installation [version] or SQL Server Database.
8. View/note any product version and identifiers (in parentheses to the right of the version).
9. To add a SQL Server Installation posture to the Asset posture:
   - Follow steps 6 and 7 under Available
   - Expand the SQL Server Installation [version] and click the >> button to move the selections under Selected.
   - When prompted for an identifier, enter the SQL Server instance name.
   - Save the posture (until the SQL Server installation postures are saved, database posture creations assigned to this SQL Server installation will fail)

Prompts for identifiers and parents will be displayed underneath the selected box.

10. To add a SQL Server Database posture to the Asset posture:
    - Follow steps 6 and 7 under Available

- Expand the SQL Server Database [version] and click the >> button to move the selections under Selected
- When prompted for a parent identifier, enter the SQL Server installation name
- When prompted for an identifier, enter the SQL Server database name; or click on the add hyperlink icon to add the identifier, and enter the SQL Server database name
- Repeat for each database defined for the installation
- Save the posture (Click on the Save icon in the middle of the bottom of the screen)

Manually entering review results into VMS (For System Administrators):

- From the left navigation frame on VMS 6, expand Asset Finding Maint[enance]
- From the expanded list, select Assets / Findings
- System Administrators: Under Navigation expand By Location
- Reviewers: Under Navigation expand Visit
- Expand the location where the asset resides
- Expand Computing,
- Expand the asset where the target database is installed
- Expand the database engine or installation
- For each vulnerability listed, select the vulnerability and enter the review results, and click Save

Importing results produced by the automated scripts:

The SRR script for SQL Server produces two XML files: one contains the security review results that may be imported directly into VMS and the other contains XML to create/identify the SQL Server host asset and SQL Server VMS postures. To import an XML file, complete the following:

- In the left navigation frame, expand Asset Finding Maint.
- Select FSO Tool Import
- Click on the System Admin button.
- Select the site where the database host asset is registered as confirmed in step 1 above and click the Submit button
- Enter the path and filename of the script results xml file to be imported. For the SQL Server asset/posture creation, the file name is dbsrr-sqlserver-postures.xml. For the SQL Server review results, the file name is named VMSimport.xml.
- If the results will not import, see the Troubleshooting section later in this document.
- Manually review vulnerability statuses to ensure the results were correctly and completely imported. Any vulnerability displaying a Not Reviewed status requires a manual review.

Note: VMS 6 imports script data only for checks results with a status of O (Open) or MR (Manual Review). The script will mark any check with results that require verification with a status of "O" so that the data to be verified will be uploaded to VMS. For example, the script will add a list of accounts assigned DBA privileges to the finding details for the reviewer to validate and remove as appropriate. The reviewer may want to consider completing the manual review of checks with a status of NR prior to import to determine if some findings are Open and the finding status in the XML file marked accordingly, i.e. <FINDING_STATUS>O</FINDING_STATUS>, in order to preserve the additional data provided by the script. The XML file may be edited with any text editor. Special care should be taken when editing the XML file to prevent the introduction of XML format errors that would prevent the script from importing successfully.

Troubleshooting XML Import Problems:

1. VMS reports that the asset is not found
   - View the database XML import file using a text or html editor. Verify the HOST NAME, IP ADDRESS and MAC ADDRESS fields match those defined for the asset in VMS.

2. Asset is found and updated, but **all** findings are reported as Not Found.
   - Review in XML file:
     - <TARGET_DESCRIP> this should indicate the correct database target (home/instance/installation or database/engine) and version
     - <IDENTIFIER> this should match the identifier as provided by the user to VMS. This is either a database name or an installation/instance name.
     - <PARENT_IDENTIFIER> if a value is listed, it should match the identifier of corresponding home/instance/installation as provided by the user in VMS
     - If any of these identifiers do not match, then the correct database target has not been found and, therefore, the findings are not found for them on the asset

One method to verify that the XML matches the VMS asset and SQL Server postures is to export the XML for the asset from VMS and review the asset ELEMENT definitions against the TARGET definitions in the SRR XML import file. This will show what values VMS requires in those fields for the asset. In some cases, the script will determine the correct value (usually retrieving a database name) and in others, it will prompt the reviewer to assign a custom value.

9. Appendix D – STIG STIGID / Checklist Discrepancy List

Below is a list of general requirements listed in the Database STIG that are not directly addressed in this checklist. The Database STIG provides general guidance for all database management systems and may not relate well to a single configuration or documentation requirement for a specific product.

Database STIG Requirement	Disposition
(DG0007: CAT II) The IAO will ensure the database is secured in accordance with STIG or NSA guidance where such guidance is available for the specific database product. Where not available, the IAO will ensure the database is secured in accordance with the general security requirements provided in this STIG and with specific security guidance in this order of preference as available: *Commercially available practices from independent security organizations such as SANS, the Center for Internet Security (CIS), and the National Institute of Standards and Technology (NIST)* *Independent testing labs such as ICSA (http://www.icsalabs.com)* *Vendor security recommendations and literature*	This requirement does not apply to MS SQL Server because SQL Server is addressed in this checklist.
DG0018 not present in Database STIG V8R1.	DG0018 removed from all checks and scripts.
(DG0053: CAT II) The IAO will ensure database client software includes only database identification parameters of databases to which that user is authorized access.	This is not configurable in SQL Server.

Database STIG Requirement	Disposition
(DG0073: CAT II) The DBA will configure the DBMS to lock database accounts after three or an IAO-specified number of consecutive unsuccessful connection attempts within a 60-minute period. The counter may be reset to 0 if a third failed logon attempt does not occur before reset. Where this requirement is not compatible with the operation of a front-end application, the unsuccessful logon count and time will be specified and the operational need documented in the System Security Plan.	This is not configurable in SQL Server.
(DG0103: CAT II) The DBA will ensure database and host system listeners that provide configuration of network restrictions are configured to restrict network connections to the database to authorized network addresses and protocols.	Listeners are known as Named Pipes in SQL Server and are covered in check DM6015.
(DG0112: CAT II) The DBA will ensure DBMS data files that store DBMS system tables and other system objects dedicated to support the entire DBMS are not shared with data files used for storage of third-party application database objects.	This is not configurable in SQL Server.
(DG0113: CAT II) The DBA will ensure database data files used by third-party applications are defined and dedicated for each application.	This is not configurable in SQL Server.
(DG0126: CAT II) The DBA will configure database account passwords to be prevented from reuse for a minimum of five changes or one year where supported by the DBMS.	This is not configurable in SQL Server.
(DG0129: CAT I) The DBA will ensure all database account passwords are encrypted when transmitted across the network.	This is not configurable in SQL Server. Encryption of logins is provided by default when using SQL Server login protocols. Applications that do not use SQL Server login protocols must address the encryption requirement.

Database STIG Requirement	Disposition
(DG0134: CAT II) The DBA will configure where supported by the DBMS a limit of concurrent connections by a single database account to the limit specified in the System Security Plan, a number determined by testing or review of logs to be appropriate for the application. The limit will not be set to unlimited except where operationally required and documented in the System Security Plan.	Microsoft does not recommend limiting user connections (http://support.microsoft.com/kb/320728).
(DG0135: CAT II) For classified systems, the DBA will configure the DBMS to report to the interactive database user upon successful connection to the database the time and date of the last successful connection and the number of unsuccessful attempts since the last successful connection. Where not available in a DBMS configuration setting, a custom logon trigger or similar function is required.	This is not configurable in SQL Server.
(DG0146: CAT II) The DBA will ensure audit records include the reason for any blocking or blacklisting of database accounts or connection source locations.	This is not configurable in SQL Server.
(DG0156: CAT III) The IAM will assign and authorize IAO responsibilities for the DBMS.	IAO assignments are not covered in a Database Security Review. This requirement is listed in the Database STIG to confirm the requirement that any IAO assignment is authorized by the IAM. IAO authorizations are expected to be checked during other, higher-level reviews.
(DG0160: CAT III) The DBA will ensure database connection attempts are limited to a specific number of times within a specific time period as specified in the System Security Plan. The limit will not be set to unlimited.	This is not configurable in SQL Server.

Database STIG Requirement	Disposition
(DG0170: CAT II) The DBA will configure the DBMS to enable transaction rollback and transaction journaling or their technical equivalent to maintain data consistency and recovery during operational cancellations, failures, or other interruptions.	This is not configurable in SQL Server.
(DG0171: CAT II) The DBA will ensure interconnections between databases or other applications operating at different classification levels are identified and their communications configured to comply with the interface controls specified in the System Security Plan.	This is not configurable in SQL Server. This is listed in the STIG to notify developers to be aware of the requirement that must consider the network architecture requirements. The general requirement for communicating between systems of different classifications is addressed in the Cross Domain Solutions (CDS) STIG.
(DG0179: CAT II) Where available, the DBA will ensure the DBMS is configured to display a warning message upon interactive user connection to the DBMS that complies with Chairman of the Joint Chiefs of Staff Memorandum(CJCSM) 6510.01 Defense in Depth: Information Assurance(IA) and Computer Network Defense(CND), current as of 14 August 2006. This requirement may be fulfilled where the database user receives the warning message when authenticating or connecting to a front-end system that includes or covers the DBMS.	This is not configurable in SQL Server.
(DG0191: CAT II) The DBA will ensure credentials stored in or used by the DBMS that are used to access remote databases or other applications are protected by encryption and access controls.	This is not configurable in SQL Server.
(DG0192: CAT II) The DBA will ensure credentials used to access remote databases or other applications use fully qualified names, i.e., globally unique names that specify all hierarchical classification names, in the connection specification.	This is not configurable in SQL Server.

Database STIG Requirement	Disposition
(DG0193: CAT II) The DBA will set expiration times for non-interactive database application account passwords to 365 days or less where supported by the DBMS.	This is not configurable in SQL Server.